Diversified Reporting Services, Inc.

RPTS CARR

HIF91020

AGING TECHNOLOGY, EMERGING THREATS: EXAMINING CYBERSECURITY VULNERABILITIES IN LEGACY MEDICAL DEVICES

TUESDAY, APRIL 1, 2025

House of Representatives,

Subcommittee on Oversight and Investigations,

Committee on Energy and Commerce,

Washington, D.C.

The Subcommittee met, pursuant to call, at 10:31 a.m. in Room 2322, Rayburn House Office Building, Hon. Gary Palmer [Chairman of the Subcommittee] presiding.

Present: Representatives Palmer, Balderson, Griffith, Dunn, Weber, Allen, Fulcher, Rulli, Guthrie (ex officio); Clarke, DeGette, Tonko, Trahan, Fletcher, Ocasio-Cortez, Mullin, and Pallone (ex officio).

Also Present: Joyce; Dingell.

Staff Present: Ansley Boylan, Director of Operations; Jessica Donlon, General Counsel; Sydney Greene, Director of

Finance and Logistics; Brittany Havens, Chief Counsel; Calvin Huggins, Clerk; Megan Jackson, Staff Director; Sophie Khanahmadi, Deputy Staff Director; Kristen Pinnock, GAO Detailee; Gavin Proffitt, Professional Staff Member; Alan Slobodin, Chief Investigative Counsel; Kaley Stidham, Press Assistant; Matt VanHyfte, Communications Director; Austin Flack, Minority Professional Staff Member; Tiffany Guarascio, Minority Staff Director; Katie Kraska, Minority Law Clerk; Will McAuliffe, Minority Chief Counsel, OI; Constance O'Connor, Minority Senior Counsel; Christina Parisi, Minority Professional Staff Member; Harry Samuels, Minority Counsel; and Caroline Wood, Minority Research Analyst.

*Mr. Palmer. The Subcommittee on Oversight and Investigations will now come to order.

The chair now recognizes himself for an opening statement.

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were made before existing cybersecurity requirements were established, but they can also be newer devices that have outdated software and lack the necessary cybersecurity protections required to defend against current threats.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 United States, each housing a range of rooms and beds and an average of 10 to 15 connected devices per bed, it is clear how integral medical devices are to delivering health care in the United States.

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 is unlikely

that such vulnerabilities can be 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 risk. This is particularly true in small, rural, and under-resourced facilities, making it crucial to find practical solutions.

It is also important to recognize that the healthcare sector is one of the 16 critical infrastructure sectors in the United States and has become a significant target for cyber attacks. For example, in 2017 the global WannaCry ransomware attack severely impacted the healthcare sector. In the United States 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 big _ is a big concern because, if a medical device vulnerability is exploited, the ability for a device to help monitor, diagnose, or treat a patient can be compromised.

There is also national security concerns. On January 30

the Cybersecurity and Infrastructure Security Agency and the Food and Drug Administration released an alert about a Chinese-made patient monitor that had a hidden back door 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 healthcare sector as part of a potential large-scale cyber attack to disrupt one of our nation's critical infrastructure sectors.

Progress was made to address the legacy medical devices in 2022 with the enactment of the PATCH Act, which increased the 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.

[The prepared statement of Mr. Palmer follows:]

**********COMMITTEE INSERT**********

*Mr. Palmer. The chair recognizes subcommittee ranking member, Ms. Clarke, for five minutes for an opening statement.

*Ms. Clarke. Thank you, Mr. Chairman, and I thank our witnesses for appearing before us today and bring your expertise to bear.

However, I am deeply alarmed by the Trump Administration's announcement that the Department of Health and Human Services is DOGE's next target. HHS Secretary Kennedy has announced that he is terminating 20,000 positions and shuttering regional offices across the country, creating further chaos and turmoil for Federal employees and the people who depend on the services they provide. I have difficulty seeing how we can have a hearing about how the FDA should approach legacy medical device cybersecurity without first addressing the fact that the Trump Administration and DOGE are dismantling the very agency responsible for medical device safety.

The Trump Administration's attacks on the health and safety of the American people have already done serious damage. Proposed cuts to the National Institutes of Health grant funding for medical research, abrupt terminations of research projects already underway, and cancellations of advisory committees and review panels are stifling the scientific community.

The government's partnership with the scientific community made the United States the undisputed global leader in scientific research and innovation for decades. And now that is being recklessly destroyed. Just last week Peter Marks, who served as a critical role at FDA by overseeing the regulation of vaccines, was forced to resign. And in his resignation letter he stated that, "It has become clear that truth and transparency are not being desired by the Secretary, but rather he wishes subservient confirmation of his misinformation and lies.''

In February Elon Musk and DOGE made the first workforce cuts to HHS and other agencies across the government, targeting probationary employees. Those terminations included hundreds of new hires from the Center of Device and Radiological Health, or CDRH, who had been recruited because of their expertise in artificial intelligence and other technological fields that support a review of medical devices. It took about a week for Elon Musk to realize the value of the work these employees were doing, and many were offered reinstatements. We need to know how many employees have returned to CDRH, and which positions are still vacant. The administration has not provided us that information, despite several requests from Democratic members and staff.

After two Federal judges ruled all of the probationary employees had been fired illegally, the administration has

appealed to the Supreme Court to avoid complying with the court orders. We don't know _ we yet don't know exactly how many of the 3,500 FDA employees are expected to be fired according to Secretary Kennedy's latest announcement work on medical device cybersecurity. HHS claimed that the medical device reviewers will not be affected, but said nothing about the many officials who are not considered reviewers but do in fact support the pre-market review process and assess reports of post-market adverse events.

Securing medical devices being used in healthcare facilities and for home care every day requires coordination between the FDA, manufacturers, and providers. Congress passed an appropriations bill in 2022 that tasked FDA with improving its process to strengthen cybersecurity of medical devices to protect against malicious activity that threatens health care institutions and individual patients. Medical device manufacturers must meet enhanced cybersecurity standards in their pre-market applications to FDA, and also conduct post-market monitoring of adverse events. This process is intended to provide clarity for manufacturers and hold them accountable for the safety and effectiveness of the products they are bringing to market. The standards become completely irrelevant, however, if FDA doesn't have the capacity to assess whether applicants have met the standards.

Day by day the instability caused by the Trump

Administration is further undermining the ability of HHS divisions to carry out their public health missions. If Secretary Kennedy moves forward with the DOGE plan to cut a quarter of the HHS workforce, including the 3,500 FDA staff, any progress FDA was making on cybersecurity review would be erased. The agency will have lost the people it needs to carry out fully-informed cybersecurity reviews of devices, and patient security will suffer as a result.

This chaos is totally unnecessary. President Trump and Elon Musk are intentionally making broad, unjustifiable cuts to the HHS workforce with no regard for the consequences on the health and well-being of the American people. It is impossible to make government work well with an administration in charge that is intent on dismantling it. And unfortunately, congressional Republicans are letting the destruction happen without the slightest pushback.

I urge the majority of this committee to prioritize our oversight authority and hold hearings with administration officials responsible for these attacks on our nation's health.

[The prepared statement of Ms. Clarke follows:]

**********COMMITTEE INSERT**********

*Ms. Clarke. And with that, Mr. Chairman, I yield back.

*Mr. Balderson. [Presiding.] Thank you. The chair now recognizes the chairman of the full committee, Mr. Guthrie, for five minutes for an opening statement.

*The Chair. Thank you, Chairman Balderson, 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 healthcare infrastructure, which makes it critical to our healthcare 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 percent of connected medical devices and other Internet of Things devices in hospitals and _ have had known critical vulnerabilities. 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. This leaves a significant gap in our defenses.

And extremely concerning, and hopefully to everybody in this room, in January the Federal Government issued an alert about the discovery of a patient monitor made in China that had been with the U.S. _ in the U.S. market since 2011. The device, made by Contec 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, though we can guess what the connection is. 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 state _ Government of Alaska in 2018.

Regardless of whether the patient monitor is just a low-quality product with inadequate cybersecurity controls or, as I believe, the design was intentional, the discovery is concerning from a patient safety and national security perspective.

FDA issued a safety communication with recommendations for healthcare providers and patients on how to mitigate the risks with this device. While we thankfully have no indication of direct harm caused by the vulnerability in these patient monitors, the risk identified calls attention to the patient safety risks posed by the 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 hackers could raise dose limits without the patient's knowledge or consent.''

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, cyber security experts, and the Federal Government have been coordinating to address these risks, but the 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. I thank Chair Troy for doing this _ Troy Balderson for doing this, and this discussion will help us to continue address _ addressing the technological concerns, protect patients, and help close security gaps.

[The prepared statement of The Chair follows:]

**********COMMITTEE INSERT**********

*The Chair. Again, Chair Balderson, I appreciate this, and I look forward to hearing from our witnesses, and I yield back.

*Mr. Balderson. Thank you, Mr. Chairman. The chair now recognizes the ranking member of the full committee, Mr. Pallone, for five minutes.

*Mr. Pallone. Thank you. Thank you, Mr. Chairman. The topic of this hearing, while important during normal times, is deeply divorced from the reality that we are in.

The Trump Administration has launched an unprecedented attack on the Federal health workforce, but committee Republicans are ignoring that fact and instead examining the narrow issue of cybersecurity in legacy medical devices. In fact, at this very moment there are civil servants at HHS buildings who have shown up to do their important work but are being told that their position has been terminated. And I think they deserve much better than how they are being treated now, and this is really a shameful day for the Trump Administration.

What we really should be doing is conducting oversight of how the Department of Health and Human Services and the Food and Drug Administration are supposed to function after massive restructuring and layoff announcements. Last week HHS Secretary Kennedy announced his plan to cut 20,000 full-time employees from the department. That is 25 percent of

the agency's total workforce.

He also wants to consolidate the functions of several operating divisions. Kennedy claims that health care services will not be harmed by the dramatic downsizing, but he is wrong, and everyone who is paying any attention knows that he is wrong. You can't cut 3,000 or 3,500 employees from FDA and say to the American people that there will be no effect on their health and safety. You can't cut 2,400 employees from the Centers for Disease Control and Prevention, some of whom are working to protect the public against bird flu and measles that are actively spreading through our communities, and tell the American people everything is just going to be fine. And you can't cut 1,200 scientists from the National Institutes of Health and say that America will continue to be at the cutting edge of innovation, and developing lifesaving medical breakthroughs.

This needless destruction is already hurting people, and will only get worse unless congressional Republicans join Democrats in demanding accountability and saying enough is enough. Secretary Kennedy must testify before this committee immediately on this drastic action and how it will affect public health and safety.

And it is also inexcusable that the Republican majority has ignored committee Democrats' request for an oversight hearing on the measles outbreak that has already resulted in

2 deaths and 483 cases across 31 states and the District of Columbia. There have already been more cases of measles than was reported all of last year, and this is a disease that was declared eradicated 25 years ago. But that status is in serious jeopardy, with experts telling us the outbreak might rage on for a year.

In addition to massively downsizing the CDC that responds to outbreaks like these, Secretary Kennedy has pushed unproven treatments while stripping billions of dollars of grant funding from local health departments, including in Lubbock, Texas, which is the center of the measles outbreak.

And last week the Trump Administration pushed out Doctor Peter Marks, the FDA's top vaccine official. In his resignation, Marks wrote, and I'm quoting, "It has become clear that truth and transparency are not desired by the Secretary, but rather he wishes subservient confirmation of his mismanagement and lies.''

This is a crisis that the Trump Administration is actively making worse, and yet committee Republicans have refused to schedule a hearing on this critical issue. The American people cannot wait any longer for congressional Republicans to start holding this administration accountable. We have had numerous cybersecurity hearings over the years. We know cybersecurity in health care is a problem that needs

to be addressed. But nothing will improve if thousands of Federal employees who work to solve health challenges every day are laid off.

FDA cannot address cybersecurity vulnerabilities of legacy medical devices if cybersecurity experts at FDA are fired, and we still don't have firm details on the results of the first round of DOGE layoffs at HHS. Committee Democrats have asked multiple HHS agencies for specific details about how many employees were terminated, what programs they were working on, how many were reinstated. These are basic questions, but none of them have been answered by the Trump Administration. We are sending another letter to Secretary Kennedy today on the massive layoffs and reorganization announced last week.

It is time that this committee start getting answers from the Trump Administration, and I invite the Republican majority to exercise oversight and join us in our request for information. Maybe they will have better luck at getting some answers.

Under ordinary circumstances I would welcome a hearing on the topic of medical device safety because it is important. But I simply cannot pretend that these are ordinary circumstances. Americans are going to get hurt by President Trump and Elon Musk's recklessness, and we have a responsibility to prevent it. And that is what we should be

doing.

I just wanted to say, Mr. Chairman, you know, I am getting caretakers, doctors, constituents who are telling me that they will no longer consider advice _ medical, scientific advice _ from HHS or FDA. They think that it is not reliable. So we have gone from where at one time we were the gold standard to now where a significant number of Americans and more every day say I cannot rely on the advice. I am a doctor. If the FDA or _ and CDC tells me to do certain things, I have to assume that it is false. It is a sad situation.

[The prepared statement of Mr. Pallone follows:]

**********COMMITTEE INSERT**********

*Mr. Pallone. I yield back, Mr. Chairman.

*Mr. Balderson. Thank you, Ranking Member Pallone. That concludes member opening statements.

The chair would like to remind members that, pursuant to the rule _ committee rules, all members' written opening statements will be made part of the record. Please provide those to the clerk promptly.

We want to thank our witnesses for being here this morning and taking the time to testify before this subcommittee. You have the opportunity to give an opening statement followed by a round of questions from members.

Our witnesses today are Dr. Christian Dameff, an emergency physician _ I hope I got that correct, sir _ emergency physician and co-director of the Center for Health Care Cybersecurity at the University of California, San Diego Health.

Next is Mr. Greg Garcia, the executive director of the Health Care Sector Coordinating Council Cybersecurity Working Group.

We also have with us today Mr. Erik Decker, the vice president and chief information security officer of Intermountain Health Care.

We also have with us Ms. Michelle Jump, the chief executive officer of MedSec.

And finally, Dr. Kevin Fu, a professor in the department

of electrical and computer engineering at Khoury College of Computer Sciences, Department of Bioengineering, and Kostas Research Institute, KRI, for Homeland Security at Northeastern University.

We appreciate you being here today, and I look forward to hearing from all of you.

You are all aware that the committee is holding an oversight hearing and, when doing so, has the practice of taking the testimony under oath. Do you have any objection to testifying under oath, any of you?

Seeing no objection, we will proceed. The chair advises that you are entitled to be advised by counsel, pursuant to House rules. Do you desire to be advised by counsel during your testimony today?

Seeing none, please rise and raise your right hand.

[Witnesses sworn.]

*Mr. Balderson. Thank you. Seeing the witnesses answered in the affirmative, you are now sworn in under oath, and subject to the penalties set forth in title 18, section 1001 of the United States Code.

With that we will now recognize Dr. Dameff for five minutes to give an opening statement.

I would let all of the witnesses today also know that we have timeframes. When you see the yellow light that means you are down to almost done. And then, when you see the red

light, we would like you to wrap up, so _ in cognizance of the time.

But with that, Dr. Dameff, for five minutes to give your opening statement.

TESTIMONY OF CHRISTIAN DAMEFF, MD, MS, FACEP, EMERGENCY PHYSICIAN AND CO-DIRECTOR, CENTER FOR HEALTHCARE CYBERSECURITY, UNIVERSITY OF CALIFORNIA SAN DIEGO HEALTH; ERIK DECKER, VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER, INTERMOUNTAIN HEALTHCARE; MICHELLE JUMP, CHIEF EXECUTIVE OFFICER, MEDSEC; GREG GARCIA, EXECUTIVE DIRECTOR, HEALTH SECTOR COORDINATING COUNCIL CYBERSECURITY WORKING GROUP; 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

TESTIMONY OF CHRISTIAN DAMEFF

*Dr. Dameff. Thank you. Chairman Guthrie, Chairman Palmer, Ranking Member Pallone, Ranking Member Clarke, and distinguished members of the subcommittee, thank you for the opportunity to testify today.

My name is Dr. Christian Dameff, and I'm a practicing emergency medicine physician. I'm a little different than your typical emergency room doctor, however. I'm a hacker. I now conduct research on the patient safety impacts of cyber attacks as co-director of the UC San Diego Center for Healthcare Cyber Security.

In over my 15 years of medical training and practice, I have treated thousands of patients in over a dozen healthcare systems. I have worked at large academic medical centers and small rural hospitals. Across all healthcare settings I know this to be true: medical devices are miraculous. Doctors and nurses use them every day to restart stopped hearts, deliver lifesaving medications, and precisely target disease. At their core, many modern medical devices are just computers, and this means there will be unavoidable flaws in software and hardware, flaws that can be exploited by malicious hackers and our nation's adversaries.

The truth when it comes to the cybersecurity of medical devices is that we lack many of the basic statistics needed to understand this threat. Legacy devices are ubiquitous across our hospitals. But how many? Which types? How secure or not? These are all open questions that exist in a vacuum of data. Such is the case with Contec and the next dozen devices we find with significant vulnerabilities. No one knows how many CMS 8000s there are in U.S. hospitals or where they are.

The FDA has done a tremendous job over the last 12 years of improving the cybersecurity of medical devices. However, it is critical to understand that cybersecurity is not a solvable problem. Cybersecurity is a dynamic and ever-evolving game of cat and mouse. Attack methods of the past

have waned with improved defenses, only to be reinvented to exploit new vulnerabilities in an ever-raging virtual arms race. The modern medical devices of today are the legacy medical devices of tomorrow, and this paradigm is unlikely to change.

The financial and operational stress that rural and critical access hospitals are currently under means they are unable to invest in the latest generation of medical devices. Many are using medical devices that are no longer supported by their original manufacturers. I have personally witnessed a hospital system struggling to fix an old CT scanner and ultimately resorting to purchasing parts off of eBay because of the cost of a new scanner being prohibitive.

Financial considerations aside, many rural and critical access hospitals also lack the necessary workforce. The unique combination of cybersecurity ability and biomedical engineering talent required to properly deploy, proactively patch, and continuously protect legacy devices is scarce even in urban, heavily populated regions. I respectfully offer three recommendations for consideration.

One, national health care dependency mapping. Strategic cyber defense of our critical healthcare infrastructure requires identifying weak points in hardware, software, vendors, supply chains, cloud computing, and networks. How can we defend hospitals against malicious hackers and highly-

skilled state actors when we ourselves lack even a basic understanding of the interconnections and dependencies that sustain the overall system? I support the important work led by the Health Sector Coordinating Council to map health care's dependencies and associated risks.

Two, we need to remove barriers to security research. The progress made over the last decade on improving medical device cybersecurity is commendable, but credit must also be given to the seminal work of ethical hackers and security researchers who first demonstrated these medical device vulnerabilities. Efforts to continue to make devices available for security research should be encouraged. Legal protections for ethical hackers and security researchers acting in good faith and using coordinated research _ coordinated disclosure practices should be strengthened. Current DMCA exemptions related to medical device cybersecurity research should be made permanent to ensure the exact types of discoveries like the contact vulnerability happen again [sic].

Build and automate resilient systems. The enormous effort required not just to respond to known vulnerabilities, but proactively discover new threats and patch them at scale is hard to comprehend. Government leadership in the form of evidence-based policy development and research support, coupled with innovative technology solutions from industry

and academia, may provide the force multiplier needed to address these threats. The Universal Patching and Remediation for Autonomous Defense Upgrade Program, created by ARPA-H, provides one such example of a next-generation approach to legacy medical device cybersecurity by innovating new ways for hospitals to proactively defend their legacy devices. If successful, technologies from this program may transform how we approach medical device cybersecurity.

In conclusion, legacy medical device cybersecurity vulnerabilities threaten our ability to deliver care to our patients when it matters most. But we can make progress on this pressing challenge. I applaud the committee's leadership on this critical issue. I'm optimistic that we can improve cyber resiliency in health care, and sincerely thank you for your opportunity _ for this opportunity to share my perspective and recommendations.

[The prepared statement of Dr. Dameff follows:]

**********COMMITTEE INSERT**********

*Mr. Balderson. Thank you, sir. Thank you very much. Mr. Decker, five minutes.

*Mr. Decker. There we go. Thank you, Chairman.

TESTIMONY OF ERIK DECKER

*Mr. Decker. Chairman Palmer, Vice Chairman Balderson, Ranking Member Clarke, and members of the subcommittee, in the health sector we believe cyber safety is patient safety. I am Eric Decker, vice president and chief information security officer for Intermountain Health and former chair of the Health Sector Coordinating Council's Cybersecurity Working Group.

Intermountain is a not-for-profit integrated health system with facilities in six states: Colorado, Idaho, Montana, Nevada, Utah, and Wyoming. Thank you for the opportunity to speak on behalf of Intermountain to share the thoughts on aging technology, cyber threats, and achieving defensive resilience of our critical health sector.

I will seek to address the following questions: Who are our adversaries and how do they operate? How are we defending medical technology? How can we leverage shared defense to get better?

The health sector is a utility largely owned and operated by private entities. Yet as a society we rely on the safe and 24/7 availability of care. Thus, we must tackle this problem together, the Federal Government and the private health sector are working in close collaboration. I'd like to focus on two cyber adversarial groups: nation state

actors and organized crime.

Nation state actors are state sponsored and backed with the resources of their respective national intelligence apparatus. Their motives are primarily focused on intellectual property theft for economic gain, and positioning for advantage in case of a geopolitical conflict. To illustrate, the Five Eyes and the Cybersecurity Infrastructure Security Agency warned about Volt Typhoon, a Chinese state-backed hacking group targeting U.S. critical infrastructure to pre-position malware in anticipation of a cyber conflict. It is unknown if similar pre-positioning has occurred in medical devices.

The second adversarial group is organized crime, who generally present themselves as Russian-speaking, financially-motivated criminal actors that regularly target the health sector through ransomware attacks. These attacks can also cause disruption to medical technology.

The sophistication of the nation state and organized crime threat groups is evidenced by their ability to run cyber operations at scale. They use the tactics such as social engineering, exploitation of Internet-accessible vulnerabilities, and attacks on connected third parties. We should defend accordingly.

The good news is the health sector and the Federal Government have been actively collaborating to do so since

2018. Under the Cybersecurity Act of 2015's section 405(d) we produced the Health Industry Cybersecurity Practices Managing Threats and Protecting Patients publication, also known as HICP. HICP was aligned to the NIST cybersecurity framework and serves as a how-to guide for implementing 10 key cyber practices. It is a dedicated _ has a dedicated section focused on managing medical device security. However, in the 2024 Hospital Cyber Resiliency Landscape Analysis, another jointly-produced and freely-available study, we saw that only 55 percent of hospitals have implemented the medical device security practices recommended in HICP.

It's understandable why these practices are lagging. For example, to ensure the clinical effectiveness of medical devices, before patches can be applied they must go through rigorous quality checks and testing to ensure the device will continue to operate in a safe manner. This intrinsically introduces a time lag in patching vulnerabilities. We've made progress with incentives. As part of Public Law one 116 321, signed by President Trump in January of 2021, HICP was identified as a recognized security practice which provides relief to organizations who have adopted it in the case of a regulatory enforcement. More incentives, especially for small, rural, and under-resourced organizations, is needed.

I'd like to highlight three recommendations to establish

a better collective set of defenses, and more within my written testimony.

Number one, as of March 7, all 16 Critical Infrastructure Policy Advisory Committees were disbanded through executive order. We urgently need these reestablished so we can get back to work on securing our critical infrastructure without fear of our most sensitive vulnerabilities being publicly exposed. The Critical Infrastructure Policy Advisory Committees allow for all critical infrastructure sectors to partner with their respective Federal agencies in a protective forum.

Number two, leverage the Private Sector Clearance Program and the Cybersecurity Working Group to get more cybersecurity professionals cleared for participation. This is _ then establish a joint task force among industry, academics, and our intelligence agencies to study the very real threat of nation state actors attacking and compromising medical technology. We need to connect the dots between national security intelligence and the critical infrastructure cyber defenders.

Number three, and finally, promote the Health Sector Cybersecurity Working Group, which is free to join, and actively amplify the materials and solutions developed by this working group.

In closing, and in words of Chris Inglis, the nation's

first cybersecurity director, we must build our critical infrastructure in such a way that one would need to "beat all of us to beat one of us.''

I welcome your questions.

[The prepared statement of Mr. Decker follows:]

**********COMMITTEE INSERT**********

*Mr. Balderson. Thank you, Mr. Decker.

Ms. Jump, five minutes.

TESTIMONY OF MICHELLE JUMP

*Ms. Jump. Good morning, Mr. Chairman, Vice President Balderson _ vice chairman, excuse me _ Ranking Member Clarke, and members of the committee, thank you for inviting me to testify today on the challenges of managing security of the healthcare critical infrastructure. I'm Michelle Jump, CEO of MedSec, a compliance and technical services firm dedicated to helping medical device manufacturers and hospitals to develop and maintain more secure medical devices.

While our organization is not large, our footprint is. Taken together, the combined revenue of our clients represents over 70 percent of the global market. We partner with these clients to develop their product security programs, navigate their regulatory goals, and perform penetration tests on their devices.

Prior to this I worked as a regulatory expert within various large medical device companies. I've also spent the last 15 years working in both domestic and international standards to drive better practices. I've made it my life's goal to support this work, and have been witness and a contributor to the significant gains that we've achieved and to make _ to make medical devices safer and more secure for the patients and users who depend on them.

One of my specific areas of specialty is risk

management. As such, I am glad to see the committee focusing on this important issue today. Over the past 12 years I've seen the industry take great strides in the pursuit of more secure devices.

When the FDA released its first pre-market cybersecurity guidance back in 2013, very few medical device manufacturers employed dedicated cybersecurity engineers, nor did they have other staff focused on this particular challenge. As larger medical device manufacturers started investing in focused cybersecurity programs, they began speaking out and sharing best practices. FDA's initial efforts brought this group of stakeholders together and hosted workshops. While the first FDA meeting back in 2014 fit into a small room _ I was there _ the one in 2016, it filled an entire conference hall. Today the FDA bar for cybersecurity is the highest in the world, and new laws from Congress have enabled the FDA to enforce cybersecurity on its own merit. This has driven the most effective push for cybersecurity compliance that I've seen in my career.

There's one point that I'd like to successfully convey in my testimony today, and that is that people and process are as much of this issue as a technical one. While the regulatory oversight may be impactful in driving the industry to do better, we can't regulate ourselves out of this issue. While new technology, better encryption, powerful tools

continue to become available, this will not solve our problem completely. We don't have enough skilled people with security knowledge to help protect the patients and care systems from the growing cybersecurity threats.

Another significant driver of the legacy issue is that medical devices are built using numerous software components, many of which are developed and maintained by third-party vendors. These may include commercial operating systems, communication protocols, and open source libraries. While these components enable innovation and efficiency, they only often _ they are often only supported by these component developers for a limited amount of time. Once that support ends, the component and therefore the medical devices become increasingly difficult to secure. This creates a mismatch: medical devices _ used in clinical environments to 10, 15, or 20 years, but their underlying software components may only be supported for a fraction of the time. As a result, devices that were secure at launch become vulnerable.

It is not just the medical devices that are vulnerable, but the whole health care infrastructure, which is not regulated in the way that medical devices are. So why not just replace all the outdated devices, you might ask? Unfortunately, it's not that simple. Most hospitals cannot afford to replace medical devices as they age at the pace needed to keep up with these software changes and the life

cycle.

As these devices age and manufacturers end support, hospitals are often left to assume the associated risk. However, taking on this responsibility requires more than acceptance. It demands careful and proactive management. So what do we do? Manufacturers need to commit to patching as many vulnerabilities as possible, not just those that are unacceptable, and do so on a regular basis as part of maintenance. I also support hospitals leveraging the cyber performance goals to better secure their networks, and also maintain better asset inventories to know what they have to protect.

In closing, I would like to share my opinion that what I have seen develop in this space over the past 12 years, this community of stakeholders has come together to achieve great things in this space. And I think that, if provided more resources, especially for smaller and rural hospitals, this will continue, and we will hold the line on cybersecurity, but it will take effort. Thank you.

[The prepared statement of Ms. Jump follows:]

**********COMMITTEE INSERT**********

*Mr. Balderson. Thank you, Ms. Jump.

Mr. Garcia, five minutes.

TESTIMONY OF GREG GARCIA

*Mr. Garcia. Okay, Mr. Chairman, Ranking Member Clarke, members of the committee, thank you for inviting me to testify about health care and medical device cybersecurity. I am Greg Garcia, the executive director of the Health Sector Coordinating Council's Cybersecurity Working Group, or CWG. And I'm also the nation's first assistant secretary for cybersecurity and communications for the U.S. Department of Homeland Security from 2006 to '9.

The CWG is a government-recognized critical infrastructure industry council of more than 470 healthcare providers, pharmaceutical, and medical technology companies, payers, health IT entities, and government agencies. We partner with government to identify and mitigate cyber threats to health data, research systems, manufacturing, and, most importantly, patient care. The CWG membership collaboratively develops and publishes free health care, cybersecurity leading practices and policy recommendations, and we produce outreach and communications emphasizing the imperative that cyber safety is patient safety.

We're glad the committee is taking up the important issue of legacy medical device security. It is a complex issue involving technical, operational, and business interdependencies between manufacturers and health providers.

And while cyber attacks more often go through medical devices to reach other health care data than they actually target the devices for disruption, we cannot ignore the many vulnerabilities in both new and legacy devices.

But we also cannot ignore how the broader health care ecosystem is the most targeted now of all critical infrastructure sectors by both criminal gangs and nation states, as Mr. Decker attested. This fact requires a more urgent effort by public-private partnerships to protect health care systems that cannot match the fire power of nation-state cyber tradecraft.

For our own part, on medical device security alone the CWG has published five extensive cybersecurity practices that were negotiated between medical device product manufacturers and health providers. These publications guide manufacturers and health systems on how to, one, design and build cybersecurity into medical devices from the ground up, rather than bolted on later; to manage the security of medical devices as they age in the clinical environment, recognizing it is a shared responsibility; to write model terms and conditions into contracts for the sale and service of medical devices; to deliver simple and actionable and consistent cybersecurity vulnerability communications related to products or services; to respond and recover from cyber incidents that impact computer-controlled medical

manufacturing; and, still to come soon, later this spring, to safely and cost-effectively patch and update devices used in a clinical environment.

While we continue to improve on these practices, cost and operational pressures among both manufacturers and health providers continue to complicate uniform implementation. But a key point to be made is that the health sector is an interconnected, interdependent ecosystem. We cannot address the security of our medical device manufacturing in a vacuum. We must scrutinize the procurement of unregulated software and components that support medical devices and other network systems, and the government needs to bolster its counter-espionage capabilities to protect America's critical infrastructure from nation-state cyber attacks.

So there are many moving parts. Fixing a flat tire won't do us much good if the steering column is loose and the oil warning light is dark. So let me summarize with recommendations relative to the importance of medical device cybersecurity.

First, we submitted to the administration yesterday a policy statement, which I would ask be entered into the record. In it we recommend initiation of a consultative process between the health sector and the government that starts with the best practices that we have developed by the sector, for the sector, and jointly with HHS. This process

would supplant one-way government regulation that presumes the best way to do things with a more deliberate pathway toward eventual requirements for minimum cybersecurity accountability. Such discussions could include, for example, recommendations that CMS review bundled payments to more thoroughly account for the expense of medical devices, and the need to keep devices patched and updated.

Development and enforcement of higher standards of secure by design, secure by default for otherwise unregulated third-party technology and service providers that sell into critical healthcare infrastructure and medical device manufacturers. This recommendation involves our national effort to diagram essential medical workflows supported by critical third-party services and functions that Dr. Dameff referred to that can cause systemic risk and cascading damage to patient care and operational resiliency if they are disrupted.

Finally, in closing, mobilization of a more reflexive government and industry intelligence, preparedness, and rapid response capability is essential for cyber events at the Federal, state, regional, and local levels, particularly against resource-constrained health systems and connected medical devices.

That concludes my opening statement, and I look forward to discussing your questions.

[The prepared statement of Mr. Garcia follows:]

**********COMMITTEE INSERT**********

*Mr. Balderson. Thank you, Mr. Garcia.

Dr. Fu, five minutes, please.

TESTIMONY OF KEVIN FU

*Dr. Fu. Good morning, Chairman Balderson, Ranking Member Clarke, and distinguished members of the committee. Thank you for the opportunity to provide testimony on the critical issue of cybersecurity vulnerabilities in legacy medical devices. My remarks today are informed by my over 30 years of working in health care and cybersecurity, despite my looking youthful, and include my previous experience as the inaugural acting director of medical device security at FDA's Center for Devices and Radiological Health.

I'm a professor at Northeastern University in Boston, Massachusetts, where I conduct fundamental cybersecurity research, I teach medical device security engineering, and I serve as the director of the Archimedes Center for Health Care and Medical Device Cybersecurity. My educational qualifications include three degrees from MIT, and today I'm speaking as an individual. All opinions, findings, and conclusions are my own and do not necessarily represent any views of my past or present sponsors or employers.

Let me make a few observations. If we fail to better manage the cybersecurity risks of legacy medical devices, the consequences are not theoretical; they are immediate and potentially life-threatening.

In 2008 I co-led a research team that wirelessly

exploited a legacy implantable defibrillator, demonstrating how an attacker could induce fatal heart rhythms wirelessly without physical contact. These are not abstract scenarios. Devices with similar insecurities remain in hospitals today. A bad actor who discovers a vulnerability could disable patient monitors during surgery, spoof vital signs in intensive care units, or hijacked infusion pumps to administer incorrect dosages. Without proactive cybersecurity measures including post-market oversight, we risk turning these lifesaving equipment into attack surfaces that endanger patient safety.

Now, a legacy medical device is one that is not merely insecure but is insecurable. Its software simply cannot be patched, it was never designed to be patched. It's the difference, in my opinion, between an unbuckled seatbelt versus a car without any seatbelts at all. Unsafe at any speed. While these devices are vital to the patient care, many lack the necessary security features to defend against modern threats. They often operate on unpatchable software and unsupported operating systems, making them vulnerable to attacks that can disrupt clinical operations or endanger patient safety. Unlike consumer smart home devices, failures in medical device cybersecurity can have life-or-death consequences.

With regards to the cybersecurity concerns of the Contec

patient monitor, in my opinion the cybersecurity flaws are likely the result of poor engineering rather than malice, although I previously suspected malice. However, a key lesson from that advisory is that the FDA's scrutiny of legacy medical devices should not simply be about pre-market, but needs to also focus on post-market risk management.

Moreover, in my testimony to this committee nine years ago I emphasized that the nation lacks an independent, large-scale testing facility such as those comparable to the NTSB, automotive crash safety testing, or the Nevada National Security Test Site for Destruction and Survivability Testing. Such proving grounds would be essential for evaluating the cybersecurity defenses of medical devices in whole-hospital environments. In my written testimony I offer several recommendations to manage these cybersecurity risks, but let me just highlight one this morning.

For patient safety and national security, I believe it's important to preserve and expand FDA's in-house cybersecurity expertise. Post-market vulnerability management requires FDA staff with deep technical expertise in cybersecurity, not just regulatory affairs. And these cybersecurity staff are crucial to national security, and are not necessarily the same as the pre-market review team. But these are often non-review staff who monitor and manage newly-discovered vulnerabilities and incidents and coordinate. These subject

matter experts are essential for evaluating the risks, working with manufacturers on coordinated vulnerability disclosures, and issuing effective guidance.

The loss of SME capacity at FDA would seriously hinder national readiness to respond to emergent threats, posing risks to national security. In my opinion, if two cybersecurity incidents were to occur simultaneously at present staffing levels as of yesterday, it's unlikely the FDA would be able to meet its congressionally-mandated duties to ensure the availability of safe and effective medical devices.

In summary, I believe that cybersecurity is not a problem, but rather it's part of the solution to protecting medical devices. It enables trust in medical technologies and ensures continuity of patient care. Legacy medical device security is spoiled milk, not fine wine. It does not age gracefully. It's lumpy.

With that, I'll end here, and I thank the committee for your leadership and bringing attention to this important problem, and I'd be happy to respond to your questions.

[The prepared statement of Dr. Fu follows:]

**********COMMITTEE INSERT**********

*Mr. Palmer. [Presiding.] I thank the witnesses for your testimony, and we will now move to questioning. I will begin and recognize myself for five minutes.

Mr. Decker, according to a research report cited in a September 2022 FBI Cyber Division Notification, as of January 2022, 53 percent of connected medical devices and Internet of Things devices in hospitals had known critical vulnerabilities. Are there updated estimates on _ of how many legacy medical devices are currently in use across the U.S. health care system?

*Mr. Decker. So I think Dr. Christian Dameff kind of mentioned this in his opening comments. The problem is actually sort of unknown, as far as how many of these devices exist, especially when we start talking about the concept of what is legacy versus what is non-legacy devices. This is an undefined term.

If we decided that it was based on the PATCH Act, and things that were _ all devices that were released post-PATCH Act, we're still very early in the phases of those devices sort of entering the market.

Now, you can _ we can estimate how many devices we think exist. So if you look at _ inside a typical hospital you have _ for any bed you have between 10 to 15, 8 to 10, 8 to 15-some devices connected to it. There's stats that show there's about 913,000 beds in the United States. So

extrapolating that, you get to about easily 10 million devices that exist. So it's a _ I mean, it's very pervasive. Lots of devices that are out there.

*Mr. Palmer. How can a cybersecurity vulnerability, when exploited in a legacy medical device, directly impact patient safety? Is that a big concern, that someone would manipulate a device to harm a patient?

*Mr. Decker. Yeah. So the devices themselves _ so we have to think of this as a connected ecosystem. So we have the ability to sort of cause damage to a device, which is _ doing that at scale is actually quite difficult to do unless there's an actor has those credentials or _ and those accesses.

These devices are also connected to systems. Systems run the devices. In large-scale attacks like ransomware attacks, what you see is intruders breaking into the environment, taking over the IT credentials that exist that IT uses to control the whole stack of health IT, and shutting down systems that they have access to, that the IT folks have access to. So if you shut down an upstream system from a medical device, then the medical device could be operating, but it's operating in a silo and stand-alone method. A charge nurse sitting in the floor monitoring the devices from a central location would be unable to monitor that, so you lose your scale.

*Mr. Palmer. Yeah. Mr. Garcia, how does the widespread use of legacy medical devices make health care sector more susceptible to cyber attacks?

And I have a particular interest in this. Is _ there have been ransomware attacks against hospitals, and I don't know that I have ever gotten a clear explanation for how those occurred. Would it _ is it possible that an entire hospital could be subject to a cyber attack because they gained entry through a medical device?

*Mr. Garcia. I think there's many different ways that hackers can get into hospitals. Through medical devices is certainly one of them. Mr. Decker highlighted three other methods. Vulnerabilities from unpatched Internet-facing devices or social engineering like email phishing, there's so many different ways that you can get into a hospital system. And where the medical devices aren't targeted so much directly, it's more about getting money out of the hospitals when you ransom the entire hospital system and all of the data and devices.

*Mr. Palmer. When you do that, Mr. Dameff, I think there _ I just wonder if there is other ways that if you had _ let's say the cyber attack occurred on the hospital. Could there be, for lack of a better way to describe it, a back flow into a medical device where they could park something that they could use later?

*Dr. Dameff. The theoretical, yet-to-be-proven example that you bring up is definitely possible.

So some of these medical devices are just computers, like are sitting right in front of you with your laptop. They can have the same type of malware on them that you could experience in just run-of-the-mill infections. Those types of cascading failures are spread through those devices to the rest of the health care system. It is definitely possible. We typically have seen hospital systems be ransomed by much easier ways.

*Mr. Palmer. Yes, but once they solve the initial attack, could they have at the same time planted something into a medical device that you don't even pick up because you have solved the main problem in the facility?

*Dr. Dameff. It's absolutely possible that a skilled adversary, someone like a state actor, could deploy advanced tactics like that to persist on a network, despite you trying to clean it up. So if a hospital's been ransomed, they think they can get rid of the infection, to have some type of foothold in a network in something like a medical device is likely possible. It depends on the medical device and, again, the sophistication of the adversary.

But then again, to just highlight, we don't even have the capability to detect those types of attacks with our normal hospitals. Our _ hospitals don't have advanced

cybersecurity staff Most of the time. They don't have these types of advanced tools. The answer to that question, is it theoretically possible, yes. Is it likely we would discover that with what we have in place across this country? The answer is no.

*Mr. Palmer. I think my time has expired. The chair now recognizes the ranking member of the committee, Ms. Clarke, for her questions.

*Ms. Clarke. Thank you very much, Mr. Chairman.

According to HHS's announcement on Thursday, it would be cutting 20,000 positions. FDA would see the largest staffing cut compared to other operating divisions: 3,500 employees will be terminated under the plan. Stripping thousands of FDA employees from their jobs all at once poses incredible risk for the public. We count on the FDA to, among other things, ensure food, drug, and device safety for the country. Top scientists at FDA and elsewhere are also resigning and being forced out by HHS leadership.

Dr. Fu, what impact could such a massive staff reduction have on the ability of the FDA to carry out its missions, including for the review, approval, and oversight of medical devices?

*Dr. Fu. I think any reduction would have a tremendous negative impact on the cybersecurity of medical devices, and the reason for that belief is because when I was the acting

director of medical device security at FDA a few years ago, it was a skeleton crew, a very small number of individuals, where it would have been already stressed at that point. I think losing any of those very capable individuals, those subject matter experts _ would be very difficult to address the next Contec kind of vulnerability or the next ransomware outage that affects at nation-scale hospitals across the country.

It's really a capacity issue, in my view. It takes very specific expertise and interdisciplinary skills to execute this, and FDA has some very qualified individuals on the cybersecurity space.

*Ms. Clarke. Very well. Thank you, Dr. Fu.

Mr. Decker, in your testimony you mentioned the FDA is a key stakeholder in securing medical devices, and the ongoing collaboration that is necessary to maximize safety. Would a depleted FDA workforce negatively affect what you see as FDA's role in improving the response to cybersecurity threats from legacy medical devices and new devices being reviewed by the FDA?

*Mr. Decker. Yes, this _ it will have an impact.

You know, this is a three-legged stool when we think about the medical technology. We talk about the manufacturers, we talk about the hospital organizations that deploy the medical technology, and we talk about the FDA who

help make sure the quality of the devices being released and managed post-market are entered into the environment. So all three parties, we have to partner together on that.

And one of the major ways we actually do that _ we used to do that _ is _ and I think we should get back to it _ is the Critical Infrastructure Policy Advisory Committee construct. All three of those parties are part of that construct. It actually allows for a lot of excellent work to happen, a lot of strategy work to happen, and, you know, potentially even policy changes that need to occur.

*Ms. Clarke. Absolutely. Thank you.

In February DOGE removed thousands of probationary employees across HHS. After outcry from stakeholders, particularly the medical device industry, DOGE reversed course, and HHS offered reinstatement to more than 200 employees it fired from FDA's Center for Devices and Radiological Health.

Our understanding is that, while many of them accepted the offer to return to work, some did not. I will reiterate that the Administration has not responded to Democrats' request for information about the status of the FDA employees who were fired and possibly rehired, so we don't know the full fallout from the first round of firings as we anticipate the next one.

Dr. Fu, does the staffing instability at the FDA

interfere with its ability to efficiently conduct medical device safety oversight, including post-market surveillance?

*Dr. Fu. Yes, I believe it does. It would be difficult with any kind of staffing reduction to manage the post-market or pre-market cybersecurity.

*Ms. Clarke. And who are the specialists at the FDA who may not be a direct reviewer of device applications, but still contribute to the pre and post-market review processes by directing assisting _ directly assisting reviewers?

*Dr. Fu. Sure. Well, there are regulatory experts who understand both the technology but also the regulatory guardrails there. I think those are a very special breed of communicators that are really important to connect with the hospitals, the law enforcement organizations, the medical device manufacturers. In order to speak that language, you need more than a scientist, you need more than a technical reviewer.

*Ms. Clarke. Very well. Well, thank you for being here today. Your expertise is invaluable.

Secretary Kennedy claims that food and drug and medical device reviewers and inspectors ignores the many other kinds of personnel that are vital to allowing reviewers and inspectors to do their jobs. With the huge cuts they have planned, there is no doubt that the entire agency will be left severely hamstrung in the aftermath. That should be

where we conduct congressional oversight immediately.

I yield back, Mr. Chairman.

*Mr. Palmer. The gentlelady yields. The chair now recognizes the chairman of the full committee, Mr. Guthrie, for five minutes for his questions.

*The Chair. Thank you, Mr. Chair, I appreciate that.

And so Mr. Decker, Ms. Jump, so we are talking about back-door medical device and what that means, and the discovery, and what vulnerabilities that has, and how it is concerning. So how often do we find this type of thing, Mr. Decker and Ms. Jump, if you know?

*Mr. Decker. Well, within medical devices specifically, it's unknown. You know, there was that report that came out about the Contec Chinese device. And in your opening comments you mentioned there's two potential opportunities for that to occur.

We know that there _ we know that certain nation-state adversaries are pre-positioning themselves into critical infrastructure, and other critical infrastructure have been targeted for this. So it's certainly within the realm of possibility that that's occurring within healthcare.

*The Chair. Okay. Ms. Jump?

*Ms. Jump. Thank you. I would say that, as a risk management expert, I think that, with the increased enforcement of risk management efforts, pen testing, threat

modeling that FDA has placed on manufacturers not only for new devices but also for any devices going in for a significant change of modification _ so older devices do still go through this process _ that manufacturers are being forced to actually look critically at their devices across the whole spectrum, the entire threat landscape of that device.

And therefore, I think that we are going to find more and more of these. I _ certainly with my clients I'm a risk management expert. We do threat modeling, we do pen testing, and we help those manufacturers find those issues before they become problems and start causing issues within the healthcare industry. So _

*The Chair. When you say you find these, are they mostly Chinese, or are they other countries? Are they other countries of origin?

*Ms. Jump. In _ I would _

*The Chair. Any kind of back door _

*Ms. Jump. No source, really, the manufacturers. Typically, vulnerabilities are not necessarily anything but design issues that people have gotten creative and figured out how to break the original design to do things that are malicious, right?

We are _ this is fighting _ what we're doing is we're fighting problems against a targeted group of people,

regardless of where they are on the globe, and they have various reasons. As Mr. Garcia mentioned, sometimes it's financial ransomware. If they can shut down a hospital, they can make money doing that. Sometimes it's just to disrupt. Critical infrastructure is a scary place. And if we don't feel safe going to get health care, that can cause a problem and it can cause disruption in a society.

*The Chair. But it is also for espionage as well, right?

*Ms. Jump. Sure, yeah.

*The Chair. So if you were NIH, would you buy medical equipment from China like, say, diagnostic equipment or any other medical devices?

*Ms. Jump. I'm not sure I could speak for being in a hospital environment and what I would purchase.

*The Chair. Well, a Federal Government. Would _ do you think it would be more _ I would assume, if you are China, you are an adversary like China, you are looking more _ well, I don't know what they look for.

*Ms. Jump. Sure.

*The Chair. You know what is going on with TikTok, right?

So the question is, do you think _ and I believe, if I am accurate _ at least I have been told that our governmental institutions do buy medical equipment from China, the Federal

Government, we are a little concerned about. Would you be concerned about that?

*Ms. Jump. Well, first of all, if I was in that position, I would make sure that I was purchasing devices that have recently gone through the FDA's oversight, right, some kind of submission. Because if you've gone through the FDA in the last two years, you are under a much higher scrutiny and a much higher bar than you ever would have.

Also, if you're going to be selling into the government, there is an additional bar of excellence that you have to meet in order to achieve that. So any device, regardless of where it's purchased, if they can get through those levels of review and acceptance, I would feel comfortable with those devices.

*The Chair. Okay, thanks.

Mr. Decker, anybody else want to kind of _ so you are right. So you have the ransomware issue, and then you have the espionage issue that we are concerned about.

Dr. Fu?

*Dr. Fu. I think there are examples that you do need to worry about. In particular, don't forget the cloud. Many medical devices now use cloud technology, and they're just like any other computer, as has been stated. For example, there are _ there is published reports on nation-states compromising what's known as the certificate authority.

These are the key managers of the world. And those also affect medical devices. There have been nation-state-backed ransomware that brought down cancer radiation therapy devices.

So a government entity might be purchasing a medical device, and they might not even realize there's technology from country X or country Y on the inside, and the manufacturer might not know, as well.

*The Chair. Okay. Well, thank you. Well, with just 15 seconds left I really can't get to my next question, so I will yield back and I appreciate the witnesses for being here. This is very concerning, and we are going to be on top of it.

I yield back.

*Mr. Palmer. The gentleman yields. The chair now recognizes the ranking member of the full committee, Mr. Pallone, for five minutes for his questions.

*Mr. Pallone. Thank you, Mr. Chairman.

The staffing and funding cuts being implemented at HHS are going to have serious consequences for health care across the nation, and if we are going to be able to respond effectively to health crisis today and the future, we need a strong, experienced workforce at HHS and resources devoted to risk mitigation and preparedness, enabling rapid action when it is needed.

So I wanted to ask Dr. Fu, how did the cybersecurity experts and other subject matter experts support the medical device reviewers?

And how might the speed and quality of device reviews suffer without that expertise on hand, if you will?

*Dr. Fu. So there are several experts at the table, I think, who can opine on this, as well. The _ it's _ there's a council of _ I would say a council of elders who've been through special cybersecurity training who helped to bring more consistency to the cybersecurity reviewing process. I think that's one way to describe it at the high level.

But it's really important to both have that rigor to ensure the controls are in place to manage those cybersecurity risks, but also to be consistent. And that's very important for the manufacturers to ensure that consistency across product lines and such.

*Mr. Pallone. All right, let me ask you also, my understanding is that individuals with expertise in cybersecurity and artificial intelligence _ both have _ both are needed to examine medical devices, and that those people are in very high demand. So are you concerned that the way the administration is treating Federal employees _ you know, I talked about how some were fired today when they just showed up for work _ are you concerned at all that the way the administration is treating Federal employees will harm

FDA and HHS's ability to recruit and retain this top talent that is very much in demand, if you will?

*Dr. Fu. I think it will be very difficult for FDA to recruit and retain the type of qualified individuals you'll need for this very specialized, specialized work. Cybersecurity and medical devices, you won't find too many people who study this in school or even do it in the industry.

So the people I've met and worked with at the FDA during my time were highly dedicated public servants, patriots. And I think, by and large, they did it because they felt it was good for the country. And no one is going into public service for a great salary, so I think it will be very difficult when _ in the current climate.

*Mr. Pallone. I appreciate that. And let me say, you know, I have a lot of concerns about not only what Secretary Kennedy is doing with these firings, but the indiscriminate nature of this downsizing.

And I don't want to repeat _ I know, Chairman Guthrie, we had this exchange in the other committee, in the Health Subcommittee _ because he said that, you know, he was hopeful, I guess, that all this would _ you know, all these firings and downsizing would lead to a more efficient agency, whether it was the FDA or the HHS or whatever. And my concern is that I haven't seen that.

In other words, it seems like it is very indiscriminate. There is no indication that this is being done in a way that is going to be more efficient, and that is why we need to have a hearing on what is happening with these firings. And he _ I think he said that he was willing to do that at some point, and I am going to follow up on it.

But what I said at the other hearing also was that _ and I think you are hinting at it _ is that what I am hearing from industry _ you talked about certainty, right? You know, they always worry in industry, whether it is, you know, medical devices, dietary supplements, you know, prescription drugs, that there is good and bad actors, right, and that if you are a good actor, you want certainty. You don't want, you know, the bad actors to sell things that, you know, are not safe or are not actually going to help out.

So just _ we have got 45 seconds. Just talk about the importance of certainty with industry because _ and the dangers, if you will, of, you know, not having people that you can rely on FDA anymore. The _ if you would in 30 seconds or so.

*Dr. Fu. Okay, I'll try. So there are many different kinds of certainty. There's technical certainty. We'll never have 100 percent certainty of cybersecurity, and that's something we have to accept. But the industry, FDA, they understand how to do the risk management of that and get it

to tolerable levels.

On the business front, medical device manufacturers, many of whom are part of my research center, care deeply about the consistency of reviewing as well as the certainty of what to expect. And when you have a lead reviewer suddenly disappearing, that's going to create market uncertainty of time to market, and that's going to hit the bottom line of the company if they cannot get their products to market for these lifesaving devices for patients.

*Mr. Pallone. Thank you.

Thank you, Mr. Chairman.

*Mr. Palmer. The gentleman yields.

Before I recognize Mr. Balderson I just want to point out to the committee that we recognize that there is some confusion around the modernization effort for the American people, and we have already requested a briefing from HHS so we can have a better understanding of the potential impact to our constituents.

The chair now recognizes the vice chairman of the subcommittee, Mr. Balderson, for five minutes for his questions.

*Mr. Balderson. Thank you, Mr. Chairman. Thank you again for all of you for being here today. My first question goes to Mr. Dameff.

Dr. Dameff _ I apologize, sir. What challenges do

hospitals face because of the differences between the life cycles that medical device, hardware, and software have?

*Dr. Dameff. The impacts to those hospitals are multi-factorial.

So number one, they don't have the latest and greatest medical technology in some in some cases, especially if they can't afford that. Let's think about rural critical access hospitals. Because of the financial constraints they don't have the latest generation medical devices. So any of the features that are released in these newer devices they don't have.

Two, because of the other constraints they have with staffing, expenditures, their thin margins, et cetera, these types of devices are going to persist on their networks for years and years and years until they are physically broken, for the most part. Many hospitals in this country do not have the luxury of replacing medical devices solely for cybersecurity risk concerns.

And so, as I mentioned in my testimony, there's a health system I've personally witnessed who will buy parts from the third-party secondary markets just to keep an old CT scanner going. That is a absolute legacy medical device. It is vulnerable to attack. It's running an outdated operating system. It is nearly impossible to defend without significant resources.

So these are just some of the impacts and limitations that hospitals have when it comes to these types of devices, mainly due to their financial constraints.

*Mr. Balderson. Thank you. Thank you. My next question is for you, Doctor, again, but I also want to include Mr. Decker.

Mr. Decker, can you explain why cybersecurity risks are unlikely to be sufficiently mitigated through patching and updating a device's software?

*Mr. Decker. Yes. So, as I mentioned in my testimony, there's a life cycle to the quality management of the devices themselves. So there's a time lag by when a patch can actually be released and installed on a device that has to generally be cleared through the manufacturer, be deemed safe, and then we have to deploy it into the environment and confirm that. So you might have a critical vulnerability, and that critical vulnerability may be in an IT system, can be patched within three days. It could take upwards of 30 to 60 days for that to happen inside a medical device, if it's even a certified patch.

The other thing that I would just note is the vulnerability itself is not necessarily the only problem. There's three factors that are involved in a device being exploited for harm: you have to have the vulnerability; it has to have some kind of exposure by which that vulnerability

can be accessed; and there has to be an actor that actually does something with it. So you can manage all three of those factors.

*Mr. Balderson. Thank you.

Dr. Dameff, would you _

*Dr. Dameff. I think this comes down to another thing that I tried to highlight in my testimony, which is that hospitals lack the workforce that are able to effectively mitigate these concerns. So even if there's a patch available _ miraculously, like a vulnerability been identified, the device manufacturer has made a patch _ it still has to be deployed. And these devices are sometimes in the most sensitive and time-critical parts of the hospital: operating systems, trauma bays, emergency departments. It's sometimes not a trivial process to go and update all of those devices. You can't update it in the middle of a surgery when it's connected to a patient.

So these are some of the considerations we have, that these are critical devices, they are hard to patch at scale, and that the hospitals would far often _ or there are many hospitals that would have other constraints and concerns that staff would be used for before taking them away from their daily duties to do something like patching.

It's hard for hospitals to understand theoretical cyber risk versus seeing the things right in front of them, which

is this scanner has to work for the stroke patient. That's the number-one priority. We'll take cyber as it comes.

*Mr. Balderson. Thank you. My next question is for Mr. Decker and Mr. Garcia.

Mr. Garcia, you may lead off. How does removal of legacy medical devices that are still broadly in use present risks to patient safety and clinical operations?

*Mr. Garcia. I actually would defer to Mr. Decker on that, as I'm not involved in the operational side of protecting patients and _

*Mr. Balderson. Great.

*Mr. Garcia. _ devices.

*Mr. Balderson. Perfect, sir. Thank you.

Mr. Decker?

*Mr. Decker. So to confirm your _ the question is about how does removal of the legacy devices _

*Mr. Balderson. Yes. Yes, sir.

*Mr. Decker. So if we get a clinically effective device that is patchable and has security baked in by design, then one would surmise that that's going to make it a better clinically effective device that has, you know, better security associated to it.

But that _ those elements _ you know, we have a fair amount of this over the last several years that has been baked in with some of the newer devices. But as we've said,

as many other witnesses have said on the panel, some of these devices are 10 years old or longer because of just the lifespan of them, as well. It's going to take 5 to 10 years for them to get cycled out.

*Mr. Balderson. Thank you very much.

Mr. Chairman, I yield back.

*Mr. Palmer. I thank the gentleman. The chair now recognizes the gentlelady from Massachusetts, Mrs. Trahan, for five minutes for her questions.

*Mrs. Trahan. Thank you to the chair, thank you to the ranking member and for our witnesses here today.

Just question for the chair. The briefing that you mentioned in your remarks, the briefing on the department, is that going to include all of us? Will that be bipartisan?

*Mr. Palmer. We will let you know.

*Mrs. Trahan. I look forward to it.

So this administration's reckless, across-the-board cuts to NIH grant awards have been described by one researcher as "the apocalypse of American science.'' While a Federal court has temporarily blocked these unlawful cuts from taking effect, the damage is already being felt. Researchers and institutions across the country are facing uncertainty, disruptions, and in some cases the threat of projects ending altogether.

In Massachusetts NIH funding supports groundbreaking

research on heart transplant risks and the potential of gene editing as a treatment for spinal muscular atrophy. And these are just two examples of the lifesaving work that could be _ that will be jeopardized by these cuts.

While NIH funding is often associated with drug development, it also plays a critical role in advancing medical devices, ensuring they are effective, they are safe and accessible to patients. Significant cuts to research grants would stifle that innovation, slow down the development of medical technologies that improve and save lives.

So Dr. Fu, what role does federally-funded biomedical research play in the development of medical devices that eventually reach our patients?

*Dr. Fu. So I do not presently take any funding from NIH, nor have I, but I have colleagues who do, and I work with companies that benefit from the discoveries at NIH.

And I would say the NIH research is extremely important for the fundamental beginning of the science and, for lack of a better term, de-risking before it becomes a business. And also understanding what therapies and diagnoses are going to be effective.

You'll find a lot of collaboration to ensure that the safe and effective drugs and devices will eventually reach the market, but it takes a huge amount of effort in order to

sort out the effective from the less effective.

*Mrs. Trahan. Yes. And how essential is federally-funded research in ensuring that medical devices enhance effectiveness, improve patient health outcomes, and uphold public safety?

*Dr. Fu. So how important is _

*Mrs. Trahan. How essential is it?

*Dr. Fu. So post-World War II, I think it would be very difficult to have it be anything but essential. It's become essential to just how America discovers new therapies and diagnostics.

I think the U.S. has historically led in that domain.

*Mrs. Trahan. If these cuts move forward, they won't just limit research; they will force some labs to close entirely. And I hope the majority does convene us in a bipartisan way to do our primary function in this subcommittee, which is oversight. Despite, you know, the nationwide impact on scientific progress, should these cuts go through, the majority should not show _ they need _ they must show interest in fulfilling our obligation for oversight.

In my district Federal research funding drives medical innovation at a leading biotech incubator, where NIH-backed projects turn early-stage ideas into real-world solutions, like you mentioned, Dr. Fu. These investments, they fuel

breakthroughs, they create high-quality jobs, and sustain the small businesses that power our region's economy. Cutting this funding will cost jobs, stall economic growth, and set back lifesaving advancements.

Federal support for biomedical research isn't just about science. It is about our nation's health, competitiveness, and security. And I think every member on this committee should oppose reckless NIH cuts and be in attendance when that briefing happens.

Thank you, I yield back.

*Mr. Palmer. The gentlelady yields. The chair now recognizes the gentleman from Virginia, Mr. Griffith, for five minutes for his questions.

*Mr. Griffith. Thank you very much, Mr. Chairman.

Ms. Jump, we have been hearing all this stuff going on, and you all know what you are talking about, and some of us have some idea of what you are talking about, but we got all these folks who will be watching this either now or some time in the middle of the night when we are the rerun on C-Span.

[Laughter.]

*Mr. Griffith. So could you give us an example of a common legacy medical device where a back door into the system may be present, but the capability of generating an alert is not?

*Ms. Jump. I'm not sure I could give you an example,

other than the _

*Mr. Griffith. Okay.

*Ms. Jump. _ the example of the Contec situation that we've been discussing. However, as has been mentioned previously from other folks on this panel, there are not a lot of ways of monitoring when this is happening, right?

So in _ from my perspective, I think it is very important that we put a lot of focus on preemptively finding these issues through risk management and testing these devices to make sure that we understand what kind of soft spots are there in the form of vulnerabilities. So whether it's a back door, whether it's another way of entering a medical device either for malicious behavior inside the medical device or for pivoting into a hospital as an easy access point, all of those aspects are there.

*Mr. Griffith. So the concern is, if you're at a hospital, they may be getting data on the population in general. Is that correct?

*Ms. Jump. There's a longstanding concern for privacy breaches in hospitals from a variety of sources. However, I'm not aware of any instance where there has been _ a back door has been the source of that like we've talked about here.

*Mr. Griffith. And then another concern might be that if _ and I heard somebody in the opening statements say that

there was a concern about, you know, a device that had been discovered. And while it might not be used that way, there was a backdoor way to maybe turn the device off so that if we found ourselves in a conflict with China or some other nation that makes some of these devices and they had a way to turn it off, they could _ along with all the other typical wartime things that are done, they could turn off a bunch of medical devices. In theory, they could turn those devices off and create chaos in the domestic scene. Is that correct? Is that one of the concerns?

*Ms. Jump. I'm not aware of that concern.

*Mr. Griffith. Somebody raised that issue.

Yes, sir, Mr. Decker, go for it.

*Mr. Decker. Yeah, I was _ I raised pre-positioning malware.

So the challenge _ so we know that that _ I mean it's been publicly announced, the Five Eyes have announced that they've done this in water and communications. We don't know if it's happening in health care. It's a largely unanswered question at this point. I think the way to answer that question is to get together with our national intelligence apparatus, with our HDOs, our Health Delivery Organizations, with the medical device manufacturers, put it under clearance, clear the entire, you know, task force and study, and actually study this problem. Bring the academics in and

see where this could occur.

The problem is on the delivery side we're unaware of the intelligence outside of what comes through the flash reports from the FBI and CISA.

*Mr. Griffith. And you mentioned Five Eyes. For the folks back home, Five Eyes is?

*Mr. Decker. Yeah, that's the five intelligence agencies: United Kingdom, United States of America, Australia, New Zealand, and Canada.

*Mr. Griffith. Canada, right.

All right, Dr. Dameff, last Congress the subcommittee saw the effects of a large cybersecurity incident with UnitedHealth. But on a smaller scale have you seen any example of an incident where vulnerabilities were not being assessed, and it contributed to patient harm or operational disruptions?

*Dr. Dameff. I think the best example of that is ransomware. It's a scourge upon health care. We are the most commonly-targeted critical health care _ or critical infrastructure for it. Those are vulnerabilities in healthcare infrastructure. They are attacked, malware and ransomware is deployed. And what we see as a consequence of that is huge, cascading failures not just at the hospitals that are infected, but also in the regions around them.

So I'll give you an example. There was a ransomware

attack in San Diego in 2021. Five hospitals went out. The adjacent hospitals to those ransomed hospitals saw huge spikes in emergency department visits, waiting times. Ambulance traffic skyrocketed. We did a follow-up study about a year later that looked at what happened to patients that had cardiac arrest, their heart stopped and they needed something like CPR. We looked at their outcomes from the same attack and saw a tenfold decrease in their survivability, just because there was a ransomware attack in the city.

These are the true, meaningful patient impacts to these types of cyber attacks. Legacy medical devices are one risk of that, but there are so many other ways that these adversaries are getting into our hospitals.

*Mr. Griffith. I appreciate that very much.

Mr. Chairman and witnesses, I think this is a very important hearing. I apologize that I had another hearing going on, and I am now being called to the floor. I usually like to sit and listen from beginning to end because I learn so much. But thank you all so much for being here and educating us on this important issue.

I yield back.

*Mr. Palmer. The gentleman yields. The chair now recognizes the gentleman from New York, Mr. Tonko, for five minutes for his questions.

*Mr. Tonko. Thank you, Mr. Chair.

A strong FDA is central to keeping patients who use medical devices safe. While FDA rigorously reviews new medical devices before they enter the market, it is important to maintain vigilance once a product is being marketed and in use.

Despite the Republicans' interest in discussing medical device security, they are turning a blind eye to Elon Musk and Secretary Kennedy's workforce reductions that will make it impossible for FDA to effectively regulate medical devices and protect patient safety. Secretary Kennedy has announced that HHS will lose 20,000 staff. More than a third of the employees that HHS plans to lay off currently work at FDA.

So Dr. Fu, can you explain what the subject matter experts in cybersecurity, device connectivity, and other technical fields contribute to the medical device review process in both pre and post-market stages?

*Dr. Fu. Sure, I'll give a go at that. So there are a number of cybersecurity experts who are not just good at the information technology, but also understanding how it affects kinetic systems, systems that move, systems that emit electricity to change your heart characteristics. You will find these both in the review staff themselves, but you will also find subject matter experts that have to bridge the divide with other constituencies, not just with the

manufacturers but also with the health care systems, with law enforcement organizations, especially when there's a suspected crime.

I would draw the attention to when I was acting director of medical device cybersecurity at FDA we witnessed the first case of patient harm from ransomware. This ransomware had infected the private cloud of a radiation therapy device company. I believe it was marketed to be able to have an uptime loss of no less than two hours a year, but it was down for six weeks because of ransomware. And having those subject matter experts to _ as that interstitial tissue to connect with all the groups was extremely important to rectify that situation and get these devices back online.

*Mr. Tonko. Well, thank you very much for that.

On this committee we have repeatedly heard from the Government Accountability Office and others of the challenges FDA faces in recruiting and retaining staff in jobs like foreign and domestic inspections and in positions requiring specialized technical skills. FDA's ability to oversee medical devices is supported by subject matter experts who can advise on the review of medical device applications which involve increasingly complex technology. We need people in these positions who know how to spot vulnerabilities that can indeed harm patient safety.

So Mr. Garcia, even the highest tech devices eventually

age. What are some of the challenges of identifying cybersecurity risks in devices already on the market?

*Mr. Garcia. Well, I think the health care sector has a very broad mandate for evaluating technology, and that includes medical devices, that includes all of the IT and communications systems and all of the software that runs them. It is a vast task.

And what we're focused on in the Sector Coordinating Council is looking at the totality of risk management requirements of the health care industry, knowing that medical devices is just one component in this broader infrastructure. So it's very difficult, and we're focused on developing best practices, leading practices in the whole range of cybersecurity functions, whether it's medical device security, whether it's supply chain cybersecurity, knowing who your third parties are. Whether it's workforce development, whether it's incident response or vulnerability patching, there's a whole range of things.

So we're focused on looking over the long term. How do we get ahead of this threat, not just today's regulatory environment, but how do we do this better?

*Mr. Tonko. Thank you.

And Dr. Fu, if the FDA loses a significant number of employees with cybersecurity and technological expertise, what would be the impact on FDA's ability to respond to post-

market discoveries of vulnerabilities or reports of safety issues?

*Dr. Fu. If you lose one, you're probably going to have a much harder time responding to simultaneous threats, which seem to be a natural course of the future. If you lose two, we might just not have a response.

*Mr. Tonko. Well, without sufficient staff and resources at FDA it will take longer for good products to become available for patient use, as well as for unsafe products to be taken off the market, and patients will be forced to suffer these avoidable consequences. Every problem that we should be trying to solve becomes infinitely worse and more dangerous as long as our Republican colleagues continue to enable this needless chaos that President Trump and Elon Musk have unleashed.

And with that, Mr. Chair, I yield back.

*Mr. Palmer. The gentleman yields. The chair now recognizes the gentleman from Texas, Mr. Weber, for five minutes for his questions.

*Mr. Weber. I thank the gentleman. I have got an interesting question for all of the panelists to start with.

Should medical device manufacturers have any liability? Is there a legal cause here that lawyers could take up and take the medical device manufacturers to task?

Doctor, we will start with you.

*Dr. Dameff. The liability of a failure of a medical device for a cybersecurity vulnerability is one that would be tricky to only pin on the device manufacturers. Because of this what we discussed previously is this kind of life cycle of a device.

Vulnerabilities can be discovered and were previously unknown. So a flaw in hardware or software may one day _ no one knows anything about it. Next day a hacker, an adversary to this country, a state actor with good cybersecurity talent may find a vulnerability. That device manufacturer would have no idea that vulnerability existed. And if they followed the standard practices and made it through FDA guidance, probably should not be held liable for something like that.

Now, let's say it's not the device manufacturer. Let's say the device manufacturer had a security control in place when it was sold, but a Healthcare Delivery Organization turned it off when they installed it, and then there was a subsequent breach. That would shift the liability to the Healthcare Delivery Organization, for instance.

What I'm trying to do is highlight that there is a _ it's not just a single point of failure. Any part across the spectrum _ device manufacturing engineering it, the hospitals deploying it, monitoring it, patching it, to the effective end of it where they have to decommission it, at any of those

failure points the liability could shift to who was the responsible party at that time.

*Mr. Weber. Have you experienced that in your _ you were with San Diego's _ you're still with San Diego Center?

*Dr. Dameff. Yes. Yes. I don't represent them currently during this hearing, but I have seen medical devices be infected with malware. I have seen those devices not function appropriately. The scale and scope of that problem is unknown. We do not know or have the capability to understand how extensive that problem is in hospitals across this country.

*Mr. Weber. But you did say that some _ there was some heart failures _ I think it was you, and _ or some of your earlier testimony, but _ and that never resulted in a legal proceeding?

*Dr. Dameff. Not to my knowledge, but there has been some case law regarding ransomware attacks on patient outcomes. There was a horrible case in Alabama where a pregnant mother was undergoing labor at a hospital under ransomware attack. It is alleged _ again, I don't know the individual details that were in court testimony, but it is alleged that the ransomware attack contributed to the death of a child.

*Mr. Weber. Okay, I am going to go to you, Ms. Jump, and ask you specifically. Should medical device

manufacturers have any liability?

*Ms. Jump. Well, I'm not a lawyer. I am a regulatory person. And I have been _ I've spent the last 15 years of my career interacting with the regulatory field. And I would just echo from my oral statement today that the regulatory bar held for medical device manufacturers today is second to none in the world. The new statutory authority that they've been given by Congress, they have been applying consistently, transparently, and rigorously.

And I feel that because, as Dr. Dameff had mentioned, the shared responsibility where a medical device manufacturers creates a product, it's put out into what is often a hostile environment in a hospital, because those environments from their _ just the way they're built, they are difficult to defend, it's difficult to say that someone has had any legal liability when there's that shared responsibility.

I think they should be held to the regulatory bar, which I think is high.

*Mr. Weber. Mr. Decker, do you agree with that?

*Mr. Decker. I also concur I'm not a lawyer. Cyber geek over here.

[Laughter.]

*Mr. Decker. So _ but it's complex. And, you know, I play a lawyer, you know, when we do contract negotiations.

We do have liability clauses that are built into these contracts. But it's a case-by-case basis as far as, like, what is actually occurring.

*Mr. Weber. Mr. Garcia?

*Mr. Garcia. Well, as Ms. Jump said, it is a shared responsibility, so you can see liability going both ways. If a health provider knows of a vulnerability that needs to be patched and it isn't patched, who is to blame?

We in the Sector Council have produced a model contract. So a lot of liability concerns are sometimes based on lack of clarity about who is responsible and accountable. So we developed a model contract. It was essentially negotiated by large medical device manufacturers and large health delivery organizations about what each side should be accountable for and that can make commitments to in both the sale and the service of medical devices. And we're now nearing conclusion of version two, which is based on how it has been implemented and lessons learned. And in this way we're going to get better clarity between the device manufacturers and the hospital systems about who is responsible and who is accountable.

*Mr. Weber. Okay, I appreciate that.

And Mr. Chairman, I yield back.

*Mr. Palmer. The gentleman yields. The chair now recognizes the gentleman from California, Mr. Mullin, for

five minutes for his questions.

*Mr. Mullin. Thank you, Mr. Chair, and thank you all for your testimony today.

The FDA's approval process for drugs and medical devices is often referred to as the worldwide gold standard. Around the world governments and regulators look to us for rigorous evaluation of safety and efficacy, which is the result of decades of investment and continuous improvement in our approval and monitoring processes.

The world of medical devices is becoming ever more complex. Devices are becoming smaller, smarter, and more capable of improving patient outcomes and treating or monitoring new conditions. But as devices become more sophisticated, we need to ensure that the FDA has the workforce and review processes that can not only keep up with the innovation, but continue to encourage it and drive it forward. This requires the retention and recruiting of real experts in cybersecurity, biology, chemistry, and numerous other fields involved in the approval and monitoring of devices. It requires reliable investment in biomedical and engineering research like through the research grants provided by the NIH.

The Trump Administration's actions are taking us in the opposite direction. Instead of leaning into our strengths, the Administration is crippling the FDA, an institution that

is a role model for the world. This will cause delays in approval for medical device companies, and potentially increase both cybersecurity and patient safety risks. This matters not only to my district, which is a hub of medical innovation, home to dozens of medical device manufacturers, but also to the broader world which relies on the lifesaving work these companies do. But their work will never see the light of day if the FDA is hamstrung.

So Mr. Decker, in your testimony, sir, you described the need for expanded partnerships between the government and industry to continue to develop best practices and ensure adequate cybersecurity. So how important is it to the device industry that the FDA maintain cybersecurity and other expertise on staff to thoroughly and efficiently and effectively evaluate devices, especially those that contain new and innovative technologies?

*Mr. Decker. Yeah, the FDA is a critical part of the Critical Infrastructure Policy Advisory Committee, that construct that allows for the Sector Coordinating Councils and the government coordinating councils to come together and partner on these issues. So it's an incredibly important factor.

*Mr. Mullin. And to Dr. Fu, same question. How important is the in-house expertise at the FDA to both the medical device industry and the safety of the American people

in examining innovative technologies?

*Dr. Fu. Just simply stated, it's extremely important, and happy to expand.

*Mr. Mullin. So I am concerned that, if we do not maintain the level of expertise and excellence at the FDA, innovation will slow as review times increase. Or, if corners are cut to speed up the review process, patient safety issues also increase.

I also worry that if we do not continue to invest in research both within and outside the Federal Government, we will totally lose our competitive edge, and patients will lose out on the benefit of medical devices that can save or improve their lives.

So I have time for one more question. Dr. Fu, if you will, how important is maintaining America's biomedical research enterprise through the NIH and other Federal funding sources to developing safe and effective medical devices?

*Dr. Fu. It's extremely important for that foundational engineering and science and medicine pre-product that was described earlier, pre-business. It's extremely important.

*Mr. Mullin. Great. And I think, with that, I will wrap. Thank you all again for your testimony.

And I yield back.

*Mr. Palmer. The gentleman yields. The chair now recognizes the gentleman from Florida, Mr. Dunn, for five

minutes for his questions.

*Mr. Dunn. Thank you very much, Mr. Chair, and I thank the witnesses for being here today.

As a medical doctor, I have seen the landscape of medical devices change dramatically throughout my time practicing. Devices are constantly becoming more sophisticated, which is better, of course, for course, for patients and providers. However, I am concerned that with the increased sophistication comes some increased risk, especially cyber risk and catastrophic, single point failures. This is demonstrated by that Contec CMS 8000 patient monitor that contained a back door connected to China.

As a member of the China Select Committee also, I am gravely concerned with the ways in which these back doors can be exploited by adversarial nations and just adversarial hackers. This vulnerability could be used to directly harm patients. It hinders the ability of the doctors to provide correct care. And, of course, if the risks are not understood, then these failures of patient care can sow panic and confusion.

Dr. Dameff, when a cyber threat for device is identified, what tools are available to inform the public and providers who may be using equipment, and do you think these tools are adequate?

*Dr. Dameff. That is a fantastic question. The parallel I'm going to draw is that when there is an adverse drug event that is discovered or a flaw in a medical device in its clinical functionality, there's a pretty well-established process to let providers know that there is an unintended side effect or a consequence of this particular drug.

In regards to providers, doctors, nurses, other folks that might be using these types of medical devices in clinical practice, to my knowledge the dissemination of information of these vulnerabilities to them is quite limited. Typically, what happens is that a medical device will have a vulnerability found. It _ that will be communicated by the device manufacturer to the relevant parties. And then the hospital systems, through their processes, will go to seek and patch those devices. To my knowledge _ and I could be mistaken _ I, as a clinician, as a doctor, have never received a notification personally that there was a cybersecurity vulnerability in a device I may have used.

The reason is that it is incredibly difficult to know where these devices actually are. In my statement, in my written and in my oral testimony, I mentioned that we do not have, as a nation, the capability to discover where these devices are, to know what their security state is. And so

then to be able to find a vulnerability in a device and then go to our country and find out how big a deal this is, that capability does not currently exist.

I support the efforts of things like sector mapping and potentially developing these capabilities so that we can answer that question of, when we find a vulnerability, where is it, how do we fix it, how do we know it's fixed. We currently don't have those capabilities.

*Mr. Dunn. Well, I thank you for that answer. You know, by the way, it mirrors my own experience, which is not cyber hacking or anything, but just point of failure on a device, and then the only people who knows that it failed, why it failed are the people who are involved in the ICU at the moment and, you know, it became sort of local lore.

A second question also to Dr. Dameff. You noted in your testimony that cutting-edge devices of today are the legacy devices of tomorrow, and I think that is a normal cycle. I don't know how you break that cycle, frankly. But, you know, as a device is in _ a legacy device that has been out there longer, more chance to hack it, come up with new things, but also, surely the new devices that have built-in back doors may pose more risk. What is your opinion on that?

*Dr. Dameff. I do appreciate the committee's focus on legacy medical devices, because that is likely the easiest for adversaries to target. But there really is not much of a

distinction between legacy medical devices and current medical devices when you consider the capabilities that our adversaries have.

Every time you've had _

*Mr. Dunn. They can get them both, huh? They don't care.

*Dr. Dameff. They can get them both. So if you have a talented team, a state-sponsored actor, for instance, and you dedicated resources towards a modern medical device by any definition, you could certainly find vulnerabilities and exploit those. And they wouldn't have to be back doors. I think back doors are a concerning thing because they imply intent, they imply being sneaky and hiding. But our adversaries don't need back doors to come in through the front door of these devices because, at their heart, with enough resources and power and talent, these are _ again, are just computers. They have flaws and weaknesses that can be exploited.

*Mr. Dunn. Well, that is sort of a frightening world you paint there. I wonder how many nights I have spent wandering around the ICU trusting all those machines. But thank you very much for your insights.

And I think I will stop there, Mr. Chairman. I do agree that this is a topic that deserves our attention. Thank you so much. Take care.

*Mr. Palmer. The gentleman yields. The chair now recognizes the gentlelady from New York, Ms. Ocasio-Cortez, for five minutes for her questions.

*Ms. Ocasio-Cortez. Thank you, Mr. Chair, and I share in the committee's concern regarding cybersecurity and legacy medical devices.

I am also worried that in the search for solutions we are also ignoring one of the biggest threats to people's privacy and public health in decades, which is the gutting of our Federal agencies that are responsible for implementing these policies.

Dr. Fu, I understand you were the first acting director of the Food and Drug Administration Center for Devices and Radiological Health, otherwise known as the CDRH. Can you tell us about the agency and its role in ensuring the safety of medical devices?

*Dr. Fu. I can give you an overview of pre-market and post-market, and maybe give you an example of an incident management.

So pre-market, it works with the FDA reviewers and the manufacturers to ensure that security is built in by design, rather than figure it out as an afterthought. And so there's regulatory guidance that's now been published after several years of effort. And so this is part of the consistency and help giving manufacturers certainty on what are the rules of

the game. Basically, the syllabus of the course.

On the post-market side the team will field reports of vulnerabilities from security researchers like Dr. Dameff. They'll handle reports from hospitals who are discovering ransomware. They'll handle influx from law enforcement. Sometimes FDA will find it on their own and then communicate with the parties.

And then there are many examples of incidents that have been managed using this interdisciplinary team approach. One, again, is the radiation therapy device that was down for about six weeks globally because ransomware broke into the manufacturer's private cloud.

*Ms. Ocasio-Cortez. Thank you.

*Dr. Fu. Yes.

*Ms. Ocasio-Cortez. Thank you. And, you know, digging into examples like that, if someone or an entity wanted to interfere with an implanted pacemaker or hijack a medical laser, is it correct to say that CDRH would be the primary agency responsible for monitoring the cybersecurity of these medical devices?

*Dr. Fu. CDRH, as well as ASPR, would be the two, I would say, organizations that would be the gateways if you discover a security incident in a pacemaker or a defibrillator.

*Ms. Ocasio-Cortez. Thank you. And I see here that in

2024 alone the FDA cleared or approved 33 medical devices and regulated more than 6,000 types of medical devices already on the market.

And Dr. Fu, to the best of your knowledge, were public health advocates calling for a reduction in the CDRH's workforce prior to February 2025?

*Dr. Fu. I'm not aware of any call for reduction.

*Ms. Ocasio-Cortez. And were medical device makers, the industry, advocating for shrinking the CDRH?

*Dr. Fu. My understanding from the industry members of my center is that they would advocate for the increase.

*Ms. Ocasio-Cortez. That is what we are seeing, as well.

And Mr. Decker, I understand that you are an executive of a health care system. Were you aware of any calls from physicians or providers to shrink the CDRH prior to February 2025?

*Mr. Decker. I was not aware of any.

*Ms. Ocasio-Cortez. Thank you. And, in fact, to your point, medical device and medtech companies were actually calling for more employees with greater specialization to the CDRH. I would like to enter that statement to the record today.

But in February, Elon Musk's team fired an estimated 700 employees from the FDA, including more than 200 employees at

the CDRH. And then days later they scrambled to unfire some of these employees because they realized what we already know, that a strong and fully-staffed FDA is better for everyone.

But there is one interesting thing in terms of some of the few people that Elon Musk sought to reinstate. They reinstated scientists that were reviewing his Neuralink device. Neuralink is a brain computer interface, a chip surgically implanted to the brain that Elon Musk has in front of the FDA. This kind of technology deserves secure safeguards and testing done by employees that aren't being held hostage right now. In fact, employees at the CDRH are reviewing the Neuralink right now.

And when we are looking at this pattern of Elon Musk with other agencies, we saw that Federal Aviation Administration workers were threatened with firings if they impeded Musk's company at SpaceX. The national relations _ the National Labor Relations Board had 24 investigations into shady labor practices at three of Musk's companies: SpaceX, Tesla, and X. And now we saw three of the top executives at the NLRB are gone.

Dr. Fu, what could be some of the risks of the politicization of some of the oversight of devices that could be reviewed at the CDRH?

*Mr. Palmer. The gentlelady's time has expired, but the

gentleman may answer the question.

*Ms. Ocasio-Cortez. Thank you.

*Dr. Fu. I would say the main risk, in my view, from my technical background, is the inconsistency in reviewing. And so _ and then that would have an impact on patients.

*Ms. Ocasio-Cortez. Thank you.

*Mr. Palmer. The chair now recognizes the gentleman from Georgia, Mr. Allen, for five minutes for his questions.

*Mr. Allen. Thank you. Thank you, Mr. Chairman. And I would like to, for the record, correct. Elon Musk has no authority to hire and fire anybody in the Federal Government. In a meeting with him two weeks ago we talked about that. We talked about how he was going about it. But he is simply an advisor. He is running algorithms in every department. He has no responsibility for firing and hiring anybody, and I think the record needs to reflect that.

The other thing is do _ obviously you all are experts in the threat here. How many _ I mean, do you know how many government agencies are involved in cybersecurity? Do you have any idea how many people are involved in cybersecurity in the Federal Government?

And then, like Mr. Decker, your hospital also has experts involved in cybersecurity. Is that correct?

*Mr. Decker. Yes.

*Mr. Allen. And the manufacturers have people involved

in cybersecurity, correct?

*Mr. Decker. Yes, they do.

*Mr. Allen. How many people is it going to take? How much money have we got to spend?

*Mr. Decker. Is that a question?

*Mr. Allen. Yes, sir.

*Mr. Decker. Yeah. So this is a people and process problem. And there _ what I will say is this. Inside health care we have been under-resourced as a national system to manage the problem.

*Mr. Allen. So you haven't had any cooperation with CISA or, you know _

*Mr. Decker. We've had cooperation with CISA, with HHS, with FDA. There's _

*Mr. Allen. Okay.

*Mr. Decker. There's many agencies that are involved in this _

*Mr. Allen. You got NSA, right?

*Mr. Decker. We have not had any specific _

*Mr. Allen. Okay, all right. You got the Cyber Center of Excellence _

*Mr. Decker. Yes.

*Mr. Allen. _ Command. It is the military. So no connection there?

*Mr. Decker. So one of the things I mentioned in my

written testimony is the connection to the national security apparatus to critical infrastructure has been a bit disconnected. Our connectivity is through our sector risk management agencies, so _

*Mr. Allen. Okay.

*Mr. Decker. _ Health and Human Services and CISA. Those have been the two main entry points into the dialog.

*Mr. Allen. Okay. So might this be a means and methods problem?

*Mr. Decker. Yes. Yeah, I think that we need to do a better job of sharing information and sharing intelligence back and forth between _

*Mr. Allen. That is just what I was told in a meeting a _

*Mr. Decker. Yeah.

*Mr. Allen. _ week ago.

*Mr. Decker. Yeah.

*Mr. Allen. The other thing I was told is we are playing defense.

*Mr. Decker. Yes.

*Mr. Allen. Just defense. We are not going on the offense, trying to stop these people from doing what they are doing. We just _ you know, we are just sitting back playing defense, and everybody _ it is a threat to everyone, every business, financial institutions, you name it. And

obviously, in health care, lives are at risk.

I mean, don't you think we need to figure this out and quit blaming each other for whatever we are doing?

I mean, the definition of insanity is doing the same thing over and over again and expecting a different result. It is insane to me that we sit here and say we can't figure this out. Should we have one group that does this and does it very well and is respected around the world? Right now we just look totally exposed.

Would any of the panel disagree with me on that?

So why don't we look for solutions, rather than blaming Elon Musk or President Trump or whoever and say let's get together and fix this problem? I am ready to do it, and we need your help, okay? And we need to fix this thing.

And with that, Mr. Chairman, I yield back.

*Mr. Palmer. The gentleman yields. The chair now recognizes the gentlelady from Colorado, Ms. DeGette, for five minutes for her questions.

*Ms. DeGette. Thank you so much, Mr. Chairman. And, you know, they say everything has been said, but it hasn't been said by everybody.

And I apologize for coming in late. I am the ranking Democrat on the Health Subcommittee. We are having _ I am sure you have all heard we are having a hearing downstairs right now, and the hearing downstairs right now is supposedly

on the reauthorization of user fee legislation to smooth the path of over-the-counter monograph drugs to market. So we have this hearing up here in O&I today around patient safety with medical devices and cybersecurity, and then we have the one downstairs.

And we really do feel like we are fiddling while Rome is burning today in the U.S. House of Representatives Energy and Commerce Committee because last week, Elon Musk and his youthful DOGE employees announced they were going to slash and burn HHS agencies, including the FDA. And then today 35 people showed up to work and they couldn't get in.

And so that is what we have all been talking about. And the reason we are talking about it is because, as someone who has been on this committee and worked on these agencies for almost 30 years now, I know Congress _ Article I of the Constitution, friends _ Congress has the legal authority to authorize and to oversee these agencies. All of us are for efficiency, all of us want to eliminate waste, fraud, and abuse. But when you just willy nilly cut 3,500 employees, it is going to not only fundamentally affect your ability to regulate industries like medical devices, it is also going to fundamentally undermine patient health and safety.

And so, you know, they said that the layoffs that they were having of the 20 percent of employees at FDA would just would not be regulators, but in fact it is going to be people

who are helping this agency perform its duties. And so I just want to ask all of you. I just want to ask all of you, going down the line, this simple question: Will a reduction of the experts at the FDA harm patient safety and innovation in device security, yes or no?

I will start with you, Dr. Dameff.

*Dr. Dameff. It is likely.

*Ms. DeGette. Mr. Decker?

*Mr. Decker. We would have to study it.

*Ms. DeGette. Do you think that reducing the experts that regulate medical devices and cyber technology could actually hurt, could actually help?

*Mr. Decker. It has the potential to _

*Ms. DeGette. Okay. I would like you to supplement _ once you investigate it, please supplement your answer to show me how it could help.

Ms. Jump?

*Ms. Jump. Yes.

*Ms. DeGette. Mr. Garcia?

*Mr. Garcia. Agreed.

*Ms. DeGette. Dr. Fu?

*Dr. Fu. Yes.

*Ms. DeGette. So all of you, except for Mr. Decker, who is going to do a study, think that reducing the experts could potentially harm safety and innovation.

Now I would like to also say that when the chairman of the full committee, Mr. Guthrie, was downstairs in the other hearing, Congressman Pallone and I asked him if he would please utilize this committee's broad jurisdiction and have an oversight hearing. And given the fact that four of the five witnesses today at this hearing have just told me that patient safety and innovation in device security could be undermined by these actions, I think this is urgent, and I would renew our request to have this hearing, and I would request to have this hearing before the April recess.

And with that I yield back.

*Mr. Palmer. The gentlelady yields. Just for clarification on the question she asked, does the entire U.S. health care system and all of its medical device manufacturers depend entirely on the expertise of HHS to protect us from cyber attacks?

Mr. Dameff?

*Dr. Dameff. No, but _

*Mr. Palmer. Okay, that's all. I just wanted a clarification.

The chair now recognizes the gentleman from Ohio, Mr. Rulli, for five minutes for his questions.

*Mr. Rulli. Well, thank you, Chairman.

Once again, the answer is never just throw more money at it. We see what happened in England with the health care

system. The answer on the opposition side is throw more money at it. I am more concerned about the blue-collar, rural county hospitals. I have lost two in my district. The rest of them are not doing well at all. And so I just think that I need to address that. So we have so many different aspects of it. So I am going to move to Mr. Garcia.

Mr. Garcia, what are the biggest challenges to rural hospitals right now in implementing FDA and Federal cybersecurity guidelines?

It seems like, with the $36 trillion deficit that America is functioning in, these rural hospitals cannot look to the Federal Government for any assistance at all.

And I know, like, whether it is in a lot of things that happen in the State of Ohio, we do shared costs, where perhaps somewhere like East Liverpool Hospital, with Marietta Hospital, with the one that is in Saint Clairsville, a lot of times they share different services as far as expertise. But as far as the cybersecurity aspect of it, we have hospitals that are actually helping the most needy people in my district in particular, which is rural America. These guys are not watching CNN and Fox News all day. All they are doing is making an honest day's work, honest day's pay, and they want a hospital they don't have to drive to Pittsburgh or Columbus to get to.

So how can we move forward where the rubber meets the

road, where we actually talk about tangible things that are going to help our constituents, instead of talking about fairy dust? What can be done to make a better cybersecurity with these medical devices that are inside my district?

*Mr. Garcia. Thank you for that question, Congressman.

The restraints on rural critical access FQHC health systems, it's all for resources, expertise, and workforce. Those are severely lacking in those health providers that are operating at zero to negative margins. Next week I expect we will be releasing a white paper with findings and recommendations of a series of interviews we did with executives of underserved, resource-constrained health systems across the country, 30 states, 40 executives asking, what are your needs, what are your stress points in cybersecurity, who's in charge?

And if you are to be held to a higher standard of cybersecurity, what's going to be meaningful support for you? Is it going to be grants, subsidies, more funding? Is it going to be training? What's going to help your constituents, your underserved providers meet their cybersecurity requirements so that they protect patient safety?

So that's coming out next week. So thank you for the question.

*Mr. Rulli. Well, you are spot on. I actually have

talked to three of the hospitals in my district about this very thing, and they were wondering if there is ever going to be, like, a blueprint or a guideline if they are under cybersecurity attack. You have to realize a lot of the IT guys are very limited that are in the brick-and-mortar at the moment. What is the action plan? You know, how do they move forward? What is the best way to approach it? And it sounds like you are sort of getting there.

*Mr. Garcia. Absolutely. And one of our biggest challenges with the Sector Coordinating Council is that we have produced now almost 30 best practices on how to do cybersecurity better. Mr. Decker was the co-chair of an initiative that created the Health Industry Cybersecurity Practices, or HICP. Volume one is specifically for small, rural critical accesses.

This is what you need to do. It's the top 10 cybersecurity controls. Our challenge is to get those resources out to those stakeholders who need them. We need to not only lead that horse to water, but get it to drink. And the water is the cybersecurity practices and the horse is the entire health care ecosystem.

*Mr. Rulli. The most refreshing answer I have heard today. Thank you so much, sir.

With that I yield my time back to the chair.

*Mr. Palmer. The gentleman yields. The chair now

recognizes the gentlelady from Texas, Mrs. Fletcher, for five minutes for her questions.

*Mrs. Fletcher. Well, thank you so much, Mr. Chairman, and thank you to all of our witnesses. I am glad to be here to hear from you this morning, and I apologize for missing some of the earlier testimony. I was in another hearing where we were also talking about some challenges in our health sector, and at FDA in particular.

And I know, though, that many of my colleagues have already mentioned during the hearing this morning their concerns about not only efforts to protect cybersecurity, but also to protect the American public writ large and the proposed cuts and changes that we are seeing at the Department of Health and Human Services.

Just this morning, as we have been sitting in hearings today, I am sure you all have heard, as we have _ we have gotten multiple reports _ that people are lined up outside of HHS around the block at the building that is just down the street, swiping their badges to see if they are still employed. Those folks are apparently going in. And if your badge swipes green, you are fine and you can go on in. And if it is red, you have been fired. That is what we are seeing happening.

And I am alarmed that what we are seeing from Secretary Kennedy, from President Trump is really undermining the

government's essential function of keeping us safe not only through these devastating staffing cuts, but by canceling important meetings of experts who regularly advise the FDA and other agencies, whether it is on all kinds of topics and issues and programs or whether it is on cybersecurity.

I know that just, I guess, February _ so not last month anymore _ but President Trump signed an executive order ending the advisory committee on long COVID and health equity. It hasn't stopped there. It has been reported they are considering ending an additional nine advisory committees at the CDC, including those that focus on the prevention and treatment of HIV, viral hepatitis, and sexually transmitted infections.

And as I understand it, FDA's medical device reviewers need to have the opportunity to consult with an array of advisers, right, to handle the workload, and that a single reviewer or team can't be experts in every single specialty required to properly assess every application without outside expertise.

And so my questions are really to be directed at you, Dr. Fu, because I want, with the time that we have left, which is about two-and-a-half minutes, if you could just talk to us about situations that you might have seen at the FDA where outside experts were brought in to advise the agency on a specific issue or device application, and how that enhanced

decision-making.

And then kind of the corollary to that, just because we are down to about two minutes, is if the FDA lays off the workforce that consults with reviewers on medical device cybersecurity and safety, what will be the effect on the review process?

Could you cover those topics with the time we have left?

*Dr. Fu. When you say bring in outside experts, do you mean hire or _ I am not _ could you clarify?

*Mrs. Fletcher. Just consultation with outside experts for _ and you can tell me better. You are the expert, not me. That is my understanding, that you have the opportunity to consult with others who might have particular expertise on either the devices or the conditions that are sought to be addressed.

*Dr. Fu. Well, FDA had been trying to convince me for 10 years to join, so they got me for a short time period.

One of the things I appreciate about the agency is that they would hold stakeholder meetings, public forums to get all input, whether it be patient _ input from patients on how they feel about medical device security and how it impacts how they feel about their treatments and diagnoses to holding _ I believe Michelle mentioned _ just hundreds of people in a room, primarily medical device manufacturers coming together to not just listen, but actually give input on what they

would like to see in these processes and what are the problems they're seeing to manufacture these devices to reach the public and sell, usually, to hospitals.

So I think bringing in experts, there's a small number that become employees at FDA. It's a very small team on cybersecurity in FDA. And what you will find, though, is that they try to use these public events to bring in _ and with HSCC and other organizations of that nature _ the International Medical Device Regulators Forum is another force multiplier to help globally bring more harmony to the regulations so that companies don't have to think cyber in 10 different dialects.

*Mrs. Fletcher. And just with the time I have left, what will happen at the FDA if the workforce that facilitates those discussions is laid off?

*Dr. Fu. I don't know what will happen. I don't _ I think it takes many years for an individual in that kind of position to build up their expertise and to really understand how to bring things together. And that's not the kind of thing you're going to learn from a textbook. So you can't simply post on LinkedIn "We need someone with 20 years experience doing this,'' it's _ it might not be possible to replace.

*Mrs. Fletcher. Thank you very much.

I have gone over my time, so, Mr. Chairman, I yield

back.

*Mr. Palmer. The gentlelady yields. The gentleman _ the chair now recognizes the gentleman from Idaho, Mr. Fulcher, for five minutes for his questions.

*Mr. Fulcher. Thank you, Mr. Chairman.

Mr. Garcia, during your verbal testimony you made a statement that surprised me a little bit, and it was that the medical device security in the industry, medical industry, if I understood you correctly, was the most targeted for cyber attacks. Did I get that right?

*Mr. Garcia. The entire health care ecosystem _

*Mr. Fulcher. Health care. So _

*Mr. Garcia. _ not just medical devices.

*Mr. Fulcher. Okay, so why health care?

I mean, we hear about the banking, right? Power grids. What is it about the healthcare industry that creates that target?

*Mr. Garcia. Yeah, I came from financial services before this, and at that time, 15 years ago, banking was the biggest target because that's where the money is. But then they started outspending the criminals.

The problem with health care is, first off, it is a widely distributed, multi-faceted ecosystem that has a lot of touch points, a lot of vulnerabilities. Secondly, there is less money to spend against cyber threats. And thirdly, it's

easy money. When you have a ransomware attack, if you are a hacker and you ransom a hospital, you are forcing the decision on the hospital _ should I pay the ransom and continue to treat patients, or should I not and run the risk of not treating patients and/or going out of business? That's why.

*Mr. Fulcher. Okay. That makes sense. I _ you know, it is a sad state of affairs, but it makes sense.

Mr. Decker, a question for you. Actually, a couple questions for you. You, as _ you noted during your testimony some recommendations. One is recommending that hospitals join a cybersecurity working group.

*Mr. Decker. Right.

*Mr. Fulcher. How would they go about doing that?

And if my hospitals in Idaho wanted to do that, how would that happen?

*Mr. Decker. Well, luckily, our executive director is at the table here, Greg Garcia.

So the Health Sector Coordinating Council Cybersecurity Working Group is the place where owners and operators of health care industries _ hospitals, clinics, medical device manufacturers, and so forth _ can freely join this organization and participate in the collaboration. We have about 470-some organizations that are members of that, but that's only a scratch of the surface of what represents the

actual totality of privately-owned critical infrastructure of health care.

*Mr. Fulcher. You also mentioned the previous law signed by President Trump, the Cybersecurity Act of 2015. This brings up a question that I want to ask you _

*Mr. Decker. Yeah.

*Mr. Fulcher. _ having to do with regulations. It is always a fine line for Congress to walk when you put regulations in place. You want them to serve a good purpose, but you don't want them to be obstacles. Would you talk about that for a minute? How do we walk that fine line, improve the regulations but not make them obstacles to progress?

*Mr. Decker. Yeah. We actually have an answer, an answer that we've been working on for the last eight years. The law that was signed in, Public Law 116-321, it took the health industry cybersecurity practices publication, HICP _ Greg referenced it earlier, I put it into my written testimony _ and it embedded it as a recognized cybersecurity practice. What it did was it incentivized the healthcare industry to adopt that. And if you adopt it, then the regulators have to consider that during any enforcement action.

So it's a carrot into the process. It wasn't a stimulus, it wasn't a financial stimulus into the hospitals,

but it was a way to say this is the path forward. How we built that, that the Health Industry Cybersecurity Practices document was a part of the consortium of the Critical Infrastructure Policy Advisory Committee. That is the HSCC, the Health Sector Coordinating Council, and the Government Coordinating Council coming together, working together to say these are the most important and impactful practices that are necessary. Everybody agrees. And when everybody agrees, it's very easy to say that should actually be the thing that we should then all do.

*Mr. Fulcher. Okay. Thank you for that.

Mr. Garcia, same question. Any further comment on that _

*Mr. Garcia. Well, I would just like to do a public service announcement. The Health Sector Coordinating Council, healthsectorcouncil.org is where your constituents can go to join the organization. We do not charge dues. And we welcome any and all health care regulated organizations to assist in our collective mission.

*Mr. Fulcher. Thank you for that.

Mr. Decker, I have only got 30 seconds left, but are there any comments you would like to make regarding the clarity of Federal cybersecurity standards?

*Mr. Decker. Yes. So we actually built, with HICP just last year, we put together the Cybersecurity Performance

Goals, which was a _ again, a jointly-provided effort which defined what needs to be done to protect against this resiliency attack, these ransomware attacks, the ways that we know the adversaries are breaking in, and how that connects to HICP and the whole how-to guide frame.

Those _ we need to be specific and clear when it comes to these standards. And we have _ again, like I said, we have built them. All we need to do is just capitalize on them.

*Mr. Fulcher. Thank you, Mr. Decker.

Mr. Chairman, I yield back.

*Mr. Palmer. The gentleman yields. The chair now recognizes the gentlelady from Michigan, Mrs. Dingell, for five minutes for her questions.

*Mrs. Dingell. Thank you, Mr. Chairman, and thanks for holding this hearing today.

As you have all heard from everybody talking, what is considered a medical device can be broad and include items ranging from a scalpel to a novel mechanical heart pump _ first used in my district at the University of Michigan. Innovation in medical devices is essential for our healthcare system's ability and to continue treating patients.

Recently I held a roundtable of researchers at the University of Michigan who receive NIH funding who are very concerned about what disruptions in funding will mean for

research and breakthroughs. They told me that one hiccup or brief pause in funding can push progress back for 40 years. Lifesaving clinical trials are on hold. Brain cancer research funding has been cut by 30 percent. And these are just examples.

Without funding, the medical community is unable to prepare the next generation of health professionals. They can't hire or promote staff, and they are looking at more layoffs. As we discuss the importance of medical device research and innovation, we have got to support the great minds and teams who are protecting our devices from the next generation of cyber attacks and vulnerabilities.

In addition to next generation of attacks, we all are dismayed at the next generation of firings at the FDA. The Trump Administration is creating tremendous uncertainty by firing and then rehiring the FDA workforce. As you know, on February 24, DOGE fired 700 employees and then had to rehire many of them back after realizing that they were important safety experts. And then last week Secretary Kennedy announced a plan to cut 3,500 employees from the FDA. Firing key drug safety officials in the name of efficiency is shortsighted, and it is not the way our healthcare system should be run, and it risks American safety.

Dr. Dameff, how is firing FDA safety employees an effective way to spur innovation and protect against cyber

crime?

*Dr. Dameff. I am uncertain as to the scope of effects that those firings would have, other than to mention what I previously stated is that it would likely impact the ability for the FDA to quickly and effectively measure and keep medical devices accountability at the point of submission.

It's been briefly mentioned on the rest of the panel as well that their function in post-market guidance, when a device is found to be vulnerable, is also not to be overstated. It could potentially impact that, as well.

*Mrs. Dingell. Thank you. We are all worried.

Now I want to turn my attention to electronic medical records. Different companies contract with health systems to create a complex web of providers that can transmit health records _ hospital records. However, there are concerns that sometimes the systems are blocking the necessary spread of information. This information blocking negatively impacts patient health and the quality of care that patients receive.

The efficient exchange of electronic health information is critically important to ensure that patients and providers alike have access to the most up-to-date information when making important health care decisions. Unfortunately, according to data reported by the Office of National Coordinator for Health Information Technology, there have been thousands of claims of information blocking that have

been submitted since April 2021. In my home state of Michigan there were 14,302 patients impacted in 13 health systems.

Dr. Fu, what is being done to address information blocking, and what can Congress do to ensure all organizations play fairly?

*Dr. Fu. So I think electronic health records are a really important topic, and it's one that I've studied in the past.

Although different from medical devices and different regulatory authorities, I _ what you're referring to, HIEs, or health information exchanges, were a major part of some of the ONC efforts from about 10 years ago, and it has improved health information exchange to some extent. But I too, even as a patient, have encountered this, where it's been impossible to get records across certain administrative boundaries. I'm not sure what to do about it in that particular space. It's not an area where I'm actively working at the moment.

But I know that in the past it was more incentive system-based. And then, as the meaningful use evolved into a more penalties, it _ was when my knowledge dropped off in that space. So I'm not sure to the full answer to that question.

*Mrs. Dingell. Well, I am out of time. I had one more

question. But you would agree that we have got a problem there, and we need to be addressing it?

*Dr. Fu. It's certainly a personal problem to me.

[Laughter.]

*Mrs. Dingell. I think it goes much broader.

Thank you, Mr. Chairman, and I yield back.

*Mr. Palmer. The gentlelady yields. The chair now recognizes the gentleman from Pennsylvania, the vice chairman of the full committee, Mr. Joyce, for five minutes for his questions.

*Mr. Joyce. Thank you, Chairman Palmer and Ranking Member Clarke, for holding this important hearing and for our panel for testifying with us here today.

As with many other sectors as technology has advanced, our healthcare system has become increasingly dependent on a variety of interconnected devices. The ability of medical devices to connect to and communicate across networks yields tremendous benefits in terms of the availability of real-time, accurate health data. This data is critical in improving patient outcomes and efficiency of care while ultimately with the goal to hopefully lower costs.

With widespread interconnectivity in such a critical and sensitive system as health care, we must be especially cognizant of the potential cybersecurity risks. I recall when I started my training as an intern at Johns Hopkins in

internal medicine we made home visits. We were given a map of east Baltimore. Today these same young interns go out and do these home visits, but they have connectivity. They have ability to take their devices with them. And they don't have to be looking at a map to find out where the patient is they are going to visit, but they bring sensitive data with them on their devices.

I would like to focus on some of the risks that exist as a health professional and patient level when dealing with potential vulnerable legacy medical devices. Dr. Dameff, as a physician and as an educator, do you feel that medical students and residents are receiving the adequate education and training regarding the potential cybersecurity risks of the devices that they utilize each and every day?

*Dr. Dameff. To my knowledge, there is not a standardized curriculum at any medical school across this country regarding the risks of digital health care up to and including cybersecurity.

*Mr. Joyce. Should there be?

*Dr. Dameff. That is a interesting question. I personally believe so, that we should be equipping our next generation of clinicians with that knowledge. It is a hard thing.

It would be argued that medical school is dense with enough information _ anatomy, physiology, pharmacology.

Those types of topics are often cited as being _ should be optional electives. My personal belief is that we can't practice modern medicine without these technologies. We had better equip our clinicians with the knowledge of what happens when they fail so they can still effectively care for their patients. The modern generation of clinicians, in my opinion, are not capable of safely caring for patients without things like the electronic health record, connected medical devices. And the old guard of doctors that were capable of caring for patients before the digital age are on their way out.

*Mr. Joyce. How can we better prepare that next generation of physicians to be aware of that legacy medical device to malfunction or to be targeted, should that _ you talked about medical students and your knowledge of inadequate preparation of that. What about residencies? What about fellowships? Shouldn't that continue? Shouldn't that be the basis, and then build on that basis?

*Dr. Dameff. That's a great question. I think it needs to continue throughout the entire medical education cycle, if you will. They _ the only education I'm familiar of _ with residents and fellows, for instance, has to do with utilizing the electronic health record and protecting data, letting them know that if they violate HIPAA, for instance, that they could be fired or _

*Mr. Joyce. Too late, then. It's too late if we are making individuals aware after the defect has already occurred. We need to be proactive, and I think we can both agree on that.

*Dr. Dameff. I agree.

*Mr. Joyce. Mr. Garcia, you referenced in your testimony how continuing decreases in Medicare physician reimbursement impact the ability of doctors to upgrade or to replace vulnerable medical technology. Especially for physicians in rural areas that I represent, and in practice, declining reimbursement can ultimately make it unsuccessful to keep the doors open, to keep that access for the patients who need them the most. And the potential costs of more secured medical devices or the consequences of cyber attack occur in rural areas, as well.

With this in mind, Mr. Garcia, would you agree that for the healthcare cybersecurity to be improved, it is important for physicians to be adequately compensated?

*Mr. Garcia. Absolutely, Congressman. We have advocated that we need positive incentives for better cybersecurity across all healthcare systems. And, you know, what better than reimbursement? Follow the money. If you have a positive incentive that says if you do better in cybersecurity, if you can replace your aging medical devices, we will improve your reimbursement. It's that simple.

*Mr. Joyce. I think you really nailed it when you talk about how important cybersecurity is. It is important across all sectors, but it is incredibly important when it comes to patients' lives and when those lives are at stake.

Moving forward, I am confident that this committee will be a leader in allowing doctors to be better informed and properly reimbursed so that they can be partners in improving cybersecurity for their patients and within their profession.

Thank you, Mr. Chairman, and I yield.

*Mr. Palmer. The gentleman yields. Seeing there are no further members wishing to ask questions, I would like to thank our witnesses again for being here today.

I ask unanimous consent to insert into the record the documents included on the staff hearing documents list.

Without objection, so ordered.

[The information follows:]

**********COMMITTEE INSERT**********

*Mr. Palmer. Pursuant to committee rules, I remind members that they have 10 business days to submit additional questions for the record, and I ask that the witnesses submit their responses within 10 days upon receipt of the questions.

Without objection, the subcommittee is adjourned.

[Whereupon, at 12:57 p.m., the subcommittee was adjourned.]