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

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

APRIL 1, 2025

Serial No. 119–15

Published for the use of the Committee on Energy and Commerce
govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
60–119 PDF WASHINGTON : 2025

COMMITTEE ON ENERGY AND COMMERCE

BRETT GUTHRIE, Kentucky
Chairman

ROBERT E. LATTA, Ohio
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
RICHARD HUDSON, North Carolina
EARL L. "BUDDY" CARTER, Georgia
GARY J. PALMER, Alabama
NEAL P. DUNN, Florida
DAN CRENSHAW, Texas
JOHN JOYCE, Pennsylvania, *Vice Chairman*
RANDY K. WEBER, SR., TEXAS
RICK W. ALLEN, Georgia
TROY BALDERSON, Ohio
RUSS FULCHER, Idaho
AUGUST PFLUGER, Texas
DIANA HARSHBARGER, Tennessee
MARIANNETTE MILLER-MEEKS, Iowa
KAT CAMMACK, Florida
JAY OBERNOLTE, California
JOHN JAMES, Michigan
CLIFF BENTZ, Oregon
ERIN HOUCHIN, Indiana
RUSSELL FRY, South Carolina
LAUREL M. LEE, Florida
NICHOLAS A. LANGWORTHY, New York
THOMAS H. KEAN, JR., New Jersey
MICHAEL A. RULLI, Ohio
GABE EVANS, Colorado
CRAIG A. GOLDMAN, Texas
JULIE FEDORCHAK, North Dakota

FRANK PALLONE, JR., New Jersey
Ranking Member
DIANA DEGETTE, Colorado
JAN SCHAKOWSKY, Illinois
DORIS O. MATSUI, California
KATHY CASTOR, Florida
PAUL TONKO, New York
YVETTE D. CLARKE, New York
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ROBIN L. KELLY, Illinois
NANETTE DIAZ BARRAGÁN, California
DARREN SOTO, Florida
KIM SCHRIER, Washington
LORI TRAHAN, Massachusetts
LIZZIE FLETCHER, Texas
ALEXANDRIA OCASIO-CORTEZ, New York
JAKE AUCHINCLOSS, Massachusetts
TROY A. CARTER, Louisiana
ROBERT MENENDEZ, New Jersey
KEVIN MULLIN, California
GREG LANDSMAN, Ohio
JENNIFER L. MCCLELLAN, Virginia

PROFESSIONAL STAFF

MEGAN JACKSON, *Staff Director*
SOPHIE KHANAHMADI, *Deputy Staff Director*
TIFFANY GUARASCIO, *Minority Staff Director*

Subcommittee on Oversight and Investigations

GARY J. PALMER, Alabama
Chairman

TROY BALDERSON, Ohio, *Vice Chairman*
H. MORGAN GRIFFITH, Virginia
NEAL P. DUNN, Florida
DAN CRENSHAW, Texas
RANDY K. WEBER, Sr., Texas
RICK W. ALLEN, Georgia
RUSS FULCHER, Idaho
MICHAEL A. RULLI, Ohio
BRETT GUTHRIE, Kentucky (ex officio)

YVETTE D. CLARKE, New York
Ranking Member
DIANA DeGETTE, Colorado
PAUL TONKO, New York
LORI TRAHAN, Massachusetts
LIZZIE FLETCHER, Texas
ALEXANDRIA OCASIO-CORTEZ, New York
KEVIN MULLIN, California
FRANK PALLONE, Jr., New Jersey *(ex officio)*

CONTENTS

Witnesses

Submitted Material

Inclusion of the following was approved by unanimous consent.

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, DC.

The subcommittee met, pursuant to call, at 10:30 a.m. in room 2322, Rayburn House Office Building, Hon. Gary Palmer (chairman of the subcommittee) presiding.

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

Also present: Representatives Joyce and 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, Oversight and Investigations; 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.

OPENING STATEMENT OF HON. GARY J. PALMER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ALABAMA

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 healthcare 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 underresourced 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:]

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

As prepared for delivery

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

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

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

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

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

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

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

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

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

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

There are also national security concerns. On January 30th, the Cybersecurity and Infrastructure Security Agency and the Food and Drug Administration (FDA) released an alert about a Chinese-made patient monitor that had a hidden backdoor that could enable remote control and data exfiltration. While the vulnerability may have been unintentional, it raised concerns and highlighted the risk of nation-state actors pre-positioning destructive malware in our health care sector as part of a potential, large-scale cyberattack to disrupt one of our nation’s critical infrastructure sectors.

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

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

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

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

Mr. PALMER. The Chair recognizes subcommittee Ranking Member Ms. Clarke for 5 minutes for an opening statement.

OPENING STATEMENT OF HON. YVETTE D. CLARKE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

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 who 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 premarket review process and assess reports of postmarket 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 healthcare institutions and individual patients. Medical device manufacturers must meet enhanced cybersecurity standards in their premarket applications to FDA, and also conduct postmarket 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 on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Oversight and Investigations Ranking Member Yvette Clarke

Hearing on "Aging Technology, Emerging Threats: Examining the Cybersecurity Vulnerabilities in Medical Devices"

April 1, 2025

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 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 U.S. 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 a critical role at FDA by overseeing the regulation of vaccines was forced to resign. In his resignation letter he stated that "it has become clear that truth and transparency are not 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 newer hires from the Center for 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 that 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 yet know exactly how many of the 3,500 FDA employees who are expected to be fired according to Secretary Kennedy's latest announcement work on medical device cybersecurity. HHS claimed that 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 premarket review process and assess reports of postmarket adverse events.

Securing medical devices being used in health care facilities and for home care every day requires coordination between FDA, manufacturers, and providers. Congress passed an appropriations bill in 2022, that tasked FDA with improving its processes 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 premarket applications to FDA and also conduct postmarket monitoring for adverse events.

This process is intended to provide better clarity for manufacturers and hold them accountable for the safety and effectiveness of the products they are bringing to the 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 this DOGE plan to cut a quarter of the HHS workforce, including 3,500 FDA staff, any progress FDA was making on cybersecurity review will be erased. The agency will have lost the people it needs to carry out fully informed cybersecurity reviews of devices. And patient safety 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 wellbeing 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.

I yield back.

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 5 minutes for an opening statement.

OPENING STATEMENT OF HON. BRETT GUTHRIE, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF KENTUCKY

Mr. GUTHRIE. Thank you, Chairman Balderson, for holding this important oversight hearing on cybersecurity vulnerabilities and 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, healthcare delivery organizations, cybersecurity 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 healthcare 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 Mr. Guthrie follows:]

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

As prepared for delivery

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

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

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

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

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

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

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

FDA issued a safety communication with recommendations for health care providers and patients on how to mitigate the risk with this device. While we, thankfully, have no indication of direct harm caused by the vulnerability in these patient monitors the risks identified call attention to the patient safety risks posed by vulnerabilities in legacy medical devices. Another example that is illustrative of these risks is that "there have been cases where insulin pumps have been hacked, and this security flaw meant that the hackers could raise dose limits without the patient's knowledge or consent."[5]

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

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

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

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

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

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

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

Mr. GUTHRIE. 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 5 minutes.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

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 healthcare 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, 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 Dr. 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 healthcare 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 on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Ranking Member Frank Pallone, Jr.

Hearing on "Aging Technology, Emerging Threats: Examining the Cybersecurity Vulnerabilities in Medical Devices"

April 1, 2025

The topic of this hearing—while important during normal times—is completely divorced from the reality 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. They deserve much better than how they are being treated, and this is a shameful day for the Trump administration.

What we should really be doing is conducting oversight of how the Department of Health and Human Services (HHS) and the Food and Drug Administration (FDA) 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's 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 it.

You cannot cut 3,500 employees from FDA and say to the American people that there will be no effect on their health and safety. You cannot cut 2,400 employees from 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 will be just fine. And you cannot 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 it 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.

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 two 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. 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 Dr. Peter Marks, the FDA's top vaccine official. In his resignation, Marks wrote, "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. 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, and 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 this Administration, and I invite the Republican majority to exercise oversight and join us in our request for information. Maybe they'll have better luck at getting 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 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. That's what we should be doing.

I have to say, Mr. Chairman, I'm getting caretakers, doctors, constituents that say they can no longer rely on medical and scientific advice from HHS or FDA. We were the gold standard and now every day doctors say, "I can no longer rely on the advice from FDA or CDC. I have to assume that it's false." It's a sad situation.

I yield back.

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 codirector 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 Healthcare 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 Healthcare.

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 5 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 5 minutes to give your opening statement.

STATEMENTS OF CHRISTIAN DAMEFF, M.D., MS, CODIRECTOR, CENTER FOR HEALTHCARE CYBERSECURITY,, UNIVERSITY OF CALIFORNIA, SAN DIEGO; ERIK DECKER, VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER, INTERMOUNTAIN HEALTHCARE; MICHELLE JUMP, CHIEF EXECUTIVE OFFICER, MEDSEC; GREG GARCIA, EXECUTIVE DIRECTOR, HEALTHCARE AND PUBLIC HEALTH SECTOR COORDINATING COUNCIL CYBERSECURITY WORKING GROUP; AND KEVIN FU, PH.D., PROFESSOR, NORTHEASTERN UNIVERSITY, AND DIRECTOR, ARCHIMEDES CENTER FOR HEALTHCARE AND MEDICAL DEVICES CYBERSECURITY

STATEMENT OF CHRISTIAN DAMEFF, M.D.

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 codirector of the UC San Diego Center for Healthcare CyberSecurity.

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.

(1) National healthcare 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 healthcare's dependencies and associated risks.

(2) 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.

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 healthcare, and sincerely thank you for your opportunity—for this opportunity to share my perspective and recommendations.

[The prepared statement of Dr. Dameff follows:]

Testimony of Dr. Christian Dameff, MD

Co-director of the UCSD Center
for Healthcare Cybersecurity

"Aging Technology, Emerging Threats: Examining Cybersecurity Vulnerabilities in Legacy Medical Devices"

**Before the Committee on Energy and Commerce
Subcommittee on Oversight and Investigations**

U.S. House of Representatives

**April 1st, 2025
Washington, DC**

Introduction

Chairman Guthrie, Chairman Palmer, and Ranking Member Pallone, distinguished members of the subcommittee, thank you for the opportunity to testify today about the cyber threats legacy medical devices pose to our great nation. My name is Dr. Christian Dameff and I am a practicing physician. I train medical students and resident doctors as an assistant professor of Emergency Medicine at UC San Diego. I am a little different than your typical emergency medicine doc, however. I am also a hacker, and following my graduation from fellowship was appointed Medical Director of Cybersecurity at UC San Diego Health, the first such position in the nation. I now conduct research on the patient safety impacts of cyberattacks as co-director of the UC San Diego Center for Healthcare Cybersecurity. I also am the co-principal investigator of the Healthcare Ransomware Response and Resilience Program, a two year research effort funded by the Advanced Research Projects Agency for Health (ARPA-H) to revolutionize hospital ransomware detection, and prototype advanced rapidly deployable replacement systems to hospitals under attack, so that they can continue to safely treat patients, even as the “normal” hospital network is being fixed.

Clinical Practice & Medical Devices

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 life-saving medicine, and precisely target disease. Over the years, as we have innovated increasingly powerful healthcare technologies, medical devices, like many other patient care tools, have become connected to networks and the wider Internet.

This capability benefits clinicians in a number of ways- we can collect more data from our patients, allowing us to make better, more personalized medical decisions. We can monitor therapies being delivered out of the hospital, allowing for patients to receive care in the comfort of their home and helping to decrease healthcare costs. We can update these devices remotely, avoiding manual effort, saving patients from cumbersome appointments and providing new functionality for these devices.

The incredible benefits medical devices bring also come with costs. At their core, modern medical devices are computers and this means that there will unavoidably be flaws in code. When flaws in code are exposed to the wider world, cybersecurity threats arise.

Our patients depend on millions of medical devices- many of them aging, machines- to deliver life-saving care. The cybersecurity of our legacy medical devices thus becomes a literal matter of life and death.

Legacy Medical Device Blind Spots

The first step to solving any public health challenge is to understand the extent of the problem. The epidemiology of disease is well known- tracking trauma or counting cancers are hard but realistic tasks. The truth when it comes to the cybersecurity of legacy medical devices is that we lack many of the basic statistics needed to understand the magnitude of the threat. Legacy devices are ubiquitous across our healthcare infrastructure but how many- which types- how secure- or not- these are all open questions existing in a vacuum of data.

No regional or national medical device inventory exists, and current assessments of the scope of the problem rely on expert opinion or limited biased data sources. Many hospitals themselves lack an internal inventory of their own medical devices, and struggle to understand the attack surface within their own four walls. Compounding this problem is that legacy medical devices that still function are not decommissioned, they are resold on the secondary market where the next healthcare provider assumes the cyber risk, and these “next” healthcare providers are often under-resourced, poorer hospitals that can’t afford to buy new. We currently don't have the capability to determine at a national scale how many and where the legacy medical devices are. Such is the case with Contec and the next dozen devices we find with significant vulnerabilities. No one knows how many CMS8000s there are in U.S. hospitals, or where they are.

The U.S. Food and Drug Administration has done a tremendous job over the last 12 years of improving the cybersecurity of medical devices across the lifecycle. Devices coming on to the market today are significantly more secure than those prior- and that is the result of intentional design and guidance. 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 categories of 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.

Broad Impacts

While the scope of the legacy medical device problem is unknown, the potential for patient safety impact when devices are compromised is crystal clear. Vulnerable legacy medical devices pose several significant risks to safe and secure healthcare delivery.

Although to my knowledge no medical device has been publicly confirmed as the first point of entry for a ransomware attack, legacy medical devices reside on sensitive hospital networks and the potential for cross-infection is high, meaning that when a hospital network is attacked, it's highly likely that medical devices will become collateral damage.

As ransomware and other cyber threats spread across a network, the likelihood of lost connectivity and disruption skyrockets. When doctors and nurses are not able to utilize network-dependent computers and medical devices, patient care suffers. A growing body of literature highlights the effects ransomware can exert over an entire region. Our research has demonstrated huge spikes in emergency department patient volumes, prolonged wait times, record high ambulance diversions, and worse outcomes from cardiac arrest when ransomware attacks occur in *neighboring* hospitals- the magnitude of impact on infected hospitals is likely even higher. The "cyber blast radius" occurring when one hospital is hit is a ripple effect impacting care across an entire geographic region.

A more ominous scenario arises if adversaries one day deliberately target specific medical devices. While such an event has not yet come to pass, the potential for sophisticated, focused attacks on highly used, highly impactful medical devices could result in widespread catastrophe. Attacks on the most commonly used infusion pumps, laboratory systems, or imaging devices- or on the cloud computing infrastructure such devices increasingly rely on- could prove catastrophic.

The simple reason for this is that medical devices are critical to providing the best care in a number of time-sensitive emergencies. When patients are fighting deadly infection, hemorrhaging from blunt trauma, or suffering from a massive heart attack, minutes - sometimes even seconds- matter. Just as CT scanners are critical for diagnosing life-threatening strokes and infusion pumps are essential to delivering precise amounts of medicine to premature babies, thousands of legacy medical devices are used in hundreds of critical clinical workflows. When doctors and nurses are not able to access these tools, patients are harmed.

Rural & Critical Access

Rural and critical access hospitals provide critically needed healthcare to local communities across the country, allowing many of our fellow citizens the chance to live healthy, productive lives. The financial and operational stress such hospitals are currently under is hard to overstate. Many such facilities are unable to invest in the latest generation of medical devices- and some may be using legacy devices no longer supported by their original manufacturer. I have personally witnessed a hospital system struggling to fix an old CT scanner and ultimately resorting to purchasing spare parts off

Ebay because the cost of a new scanner is prohibitive. The ability to replace aging- but still functional- medical devices to lessen cybersecurity risk is not a luxury many hospitals have.

Financial considerations aside, many rural and critical access hospitals also lack the necessary technical expertise needed to both mitigate device-related cybersecurity risks and more broadly defend fragile hospital networks from sophisticated cyber criminals and state actors. The unique combination of cybersecurity ability and biomedical engineering talent needed to properly deploy, proactively patch and continuously protect legacy devices is scarce even in urban, heavily populated regions. Healthcare cybersecurity professionals are a particularly rare breed amongst the larger cybersecurity workforce- itself too small a pool to meet our nation's growing needs.

Entrenchment

I hope to have illustrated that legacy medical device cybersecurity is a complex, multidimensional problem requiring our best efforts to mitigate, if not entirely solve. We face a number of obstacles in doing so- and I wish to highlight one of the main drivers of this problem- failures at the level of process and people.

Creation of cybersecurity risk in medical devices can occur at many points in the device lifecycle- from design to deployment to discontinuation- and may result from the actions of several different stakeholders. For example, medical device manufacturers may design devices using insecure software libraries or may fail to timely patch discovered vulnerabilities once devices are on the market. Hospitals may choose to procure less secure devices or fail to deploy devices securely by turning off certain settings in an effort to facilitate installation. Cybersecurity professionals may not maintain accurate device inventories (you can’t defend what you don't know you have), lack the capability to monitor devices for signs of compromise, or fail to timely patch devices to prevent attacks. A single point of failure across any of these domains with any of these stakeholders can prove fatal, if the end result is a vulnerable legacy medical device that is exploited by a cyber threat.

Device manufacturers may be best positioned to raise the baseline cybersecurity of these devices as they are the principal engineers and possess the technical information necessary to implement secure-by-design practices and techniques, but unfortunately, device manufacturers have historically engaged a reactionary approach to legacy medical devices, releasing patches, operating system updates, or end user guidance only after a problem is identified by a third party cybersecurity researcher, hacker, or adversary. In addition, it is not enough for devices to be secure sitting in a box on the hospital’s loading dock--they must be deployed and maintained securely--often in partnership with the manufacturer--by the hospital, and many hospitals, as previously discussed, still struggle to find the people, resources, and time to do so.

Recommendations

Despite understanding that improving the cybersecurity resiliency of legacy medical devices will remain a never-ending challenge, there are many important and necessary steps we must take as a nation to address this threat. I respectfully offer three recommendations for your consideration.

National Healthcare Dependency Mapping

Strategic cyber defence of our critical healthcare infrastructure requires identifying weak points in hardware, software, vendors, supply chains, cloud computing, and networks. No entity, whether commercial or governmental, currently has visibility on healthcare assets across the entire sector. How can we defend hospitals against malicious hackers and highly skilled state actors when we ourselves lack even a rudimentary understanding of the myriad interconnections and dependencies that sustain the overall system? I support the important work led by the Health Sector Coordinating Council to map healthcare's dependencies and associated sector risk.

Remove Barriers to Security Research

The progress made over the last decade on improving baseline medical device security after concerted efforts by stakeholders including the FDA and medical device manufacturers is commendable. Credit must also be given to the seminal work of ethical hackers and security researchers who first demonstrated the existence and technical proof-of-concept of medical device cybersecurity exploits. From early work on pacemaker and patient monitor security to investigations of insulin and infusion pumps, advancements in device cybersecurity first occurred when curious researchers became concerned with the cyber-safety of life-saving devices. Efforts to continue to make devices available to the security research community should be encouraged. Legal protections for ethical hackers and security researchers acting in good faith and using coordinated disclosure practices should be strengthened, including making permanent current DMCA exemptions related to medical device cybersecurity research to enable exactly the kinds of discoveries that have led to findings like the Contec vulnerability and others.

Empower People, Reduce Human Error: Build and Automate Resilient Systems

As we have established, legacy medical devices and other healthcare cybersecurity challenges arise from systemic challenges at the people and process level. To prevent cybersecurity failure we must undertake new approaches and develop new technologies that reduce dependency on fallible, human designed hardware and code. We must also scale solutions in a way that acknowledges the lack of resources, workforce, and skillset that plague many of the most vulnerable hospitals.

The enormous effort required to not just 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 technologic solutions from industry and academia may provide the force multiplier needed to surmount these existing deficiencies of resources, workflow, and skillset.

The Universal Patching and Remediation for Autonomous Defense (UPGRADE) program created by the Advanced Projects Agency for Health (ARPA-H) provides one such example of a next-generation approach to legacy medical device cybersecurity. By innovating new ways for hospitals to monitor networks and devices, rapidly identify vulnerabilities, automatically develop patches, and deploy patches at scale, UPGRADE seeks to develop new tools for hospitals to protect themselves and their patients . If successful, technologies from this program may transform how we approach medical device cybersecurity- revolutionizing the current manual, mistake-prone, human dependent status quo.

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, am optimistic that we can improve cyber resilience in healthcare, and sincerely thank you for the opportunity to share my perspective and recommendations.

Mr. BALDERSON. Thank you, sir. Thank you very much.

Mr. Decker, 5 minutes.

Mr. DECKER. There we go. Thank you, Chairman.

STATEMENT 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 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 preposition malware in anticipation of a cyber conflict. It is unknown if similar prepositioning 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 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 underresourced 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 1, 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 2, 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 3, 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:]

Intermountain Health

Testimony of

Erik Decker

Vice President, Chief Information Security Officer, Intermountain Health

on

"Aging Technology, Emerging Threats: Examining Cybersecurity Vulnerabilities in Legacy Medical Devices"

Before the

Subcommittee on Oversight and Investigations of the

Committee on Energy and Commerce

US House of Representatives

April 1st, 2025

Summary of Testimony

Chairman Guthrie, Chairman Palmer, Vice Chairman Balderson, Ranking Member Pallone, Ranking Member Clarke, and Members of the Subcommittee, I am Erik Decker, Vice President and Chief Information Security Officer for Intermountain Health, and former chairman of the Health Sector Coordinating Council's Cybersecurity Working Group (HSCC CWG). Thank you for the opportunity to speak on behalf of Intermountain Health and the health industry and provide my perspectives on aging technology, cyber threats, and achieving defensive resilience of our critical sector.

In my testimony, I will touch on the following key points:

1. The current state of adversarial cyber threats and the methods they deploy to cause damage
2. The current state of our medical device security programs and the inter-relationship with digital systems
3. Collective defense to these problems requires continual improvement in partnership between the industry and the US government.

All of this can be summarized by noting that we are all in this together. We must continue to work in partnership, with the industry improving its capabilities across all its subsectors, and the US Government improving its services to critical infrastructure, cohesion across government, supplying incentives to strengthen cyber capabilities, and where necessary, regulation that is purposeful, focused, and reflects the real world of healthcare delivery.

Introduction

Intermountain Health is a not-for-profit integrated healthcare delivery system headquartered in Salt Lake City, Utah with regional offices in Broomfield, Colorado and Las Vegas, Nevada. We are comprised of 33 hospitals – which includes our virtual hospital – more than 400 clinics, medical groups with more than 5,000 employed physicians and advanced practice providers and a health plans division called Select Health. With more than 68,000 caregivers serving over four million patients and more than one million health plan members, Intermountain provides services in six primary states: Colorado, Idaho, Montana, Nevada, Utah, and Wyoming. Our mission is to help people live the healthiest lives possible. Intermountain strives to be a model health system by partnering to proactively keep people well and providing the best possible care.

In addition to being both a provider and plan, Intermountain is also an innovation hub and has launched multiple companies seeking to address some of health care's most pressing challenges. These include companies focused on value-based care (Castell), generic pharmaceutical drugs (CivicaRx), and interoperability (GraphiteHealth). Intermountain is committed to improving community health and we are proud to be recognized as a leader in transforming healthcare by using evidence-based practices and leveraging health information technology to deliver high quality health outcomes at sustainable costs. Intermountain is actively working to accelerate the healthcare transition from volume to value. We are deeply committed to engaging in federal health policy. Intermountain Senior Vice President for Policy Greg Poulsen serves on the Medicare Payment Advisory Commission (MedPAC), and Intermountain Primary Children's Hospital Chief Medical Officer Angelo Giardino, a pediatrician, serves on the Medicaid and Chip Payment Advisory Commission (MACPAC). Intermountain also provided me the time necessary to serve for three years as the chairman of the HSCC CWG, as well as the Industry Lead for the HSCC CWG 405(d) Task Group, which developed the Health Industry Cybersecurity Practices (HICP) and the Hospital Resiliency Landscape Analysis publications.

As a critical infrastructure operator, and previous chairman of the HSCC CWG, I believe we have reached an inflection point: our adversaries are becoming increasingly sophisticated at enumerating the connectivity of our ecosystem. They have developed tried and true tactics for breaking in, just as we are becoming increasingly reliant on digital data, technology, and information sharing. We leverage digital data and technology to improve health and healthcare, to make the health workforce more productive, and to improve patient outcomes. The ability of our adversaries to monetize and capitalize on our business operations, data, intellectual property, and vulnerabilities is a significant part of the reason why the Healthcare and Public Health (HPH) Sector continues to be a prime target for cyberattacks. Ultimately, these threats have led to troubling and confirmed patient safety risks, negative impacts to public health, and a risk to national security.

Thankfully, the partnership between the HPH Sector and the US Government has matured significantly over the last several years. However, our work is never done. Despite the partnership being strong, certain parts of the HPH Sector lag on their sector-supporting cyber capabilities and must be addressed. Cyber safety is patient safety and cybersecurity is national security.

Adversarial Mindset

In 2023, the HSCC CWG and US Department of Health and Human Services assessed the hospital field and released a joint paper titled "Hospital Resiliency Landscape Analysis[1]" (aka "Landscape Analysis"). This joint effort between industry and government brought together unique insights and studied the problem of a) what's our current defensive posture to cyber threats pursuant to the Health Industry Cybersecurity Practices document (HICP[2]), and b) how are we "getting beat" by our adversaries. It was a meta-analysis that took a deep look into several industry surveys to understand our posture and

[1] Hospital Resiliency Landscape Analysis, HSCC CWG 405d Task Group, 405(d) :: Cornerstone Publications
[2] Health Industry Cybersecurity Practices, 405(d) :: Cornerstone Publications

compared that against threat intelligence sources and analysis of how the threat actors are activating. The results were very compelling, such as the integrated connectivity between hospitals, manufacturers, pharmaceutical companies, pharmacies, health plans, pharmacy benefits managers, and others, which has drastically increase the attack surface that allows for nation state and other actors to conduct their attacks.

Generally speaking, there are four groups of threat actors that cause damage to our sector. They are Nation State Actors, Organized Crime, "Hacktivists," and Insider Threats. The motivations for each of these threat actor groups are different, and it's critical that we understand those motivations as we build our defenses, ranked in order of their level of sophistication.

Threat Group	Motivations	Methods
Nation State	Geopolitical, Economic, "Cyberwarfare"	Zero-Day Attacks, highly sophisticated tools, deep supply chain attacks
Organized Crime	Monetary, Fiscal	Leverage hygiene failures, social engineering
Hacktivism	Reputational, Geopolitical	Crowd-sourcing, leveraging hygiene failures
Insider	Unintentional, Monetary	Accidental release of sensitive data, poor hygiene that enables other three attack groups

For my testimony, I will focus on Nation State Actors and Organized Crime.

Nation State Actors

To define the Nation State Actors, we need to focus on both who they are and what their motivations are. The Nation State Actors are groups that are backed by national governments, with the resources of their respective national intelligence agencies. These actors tend to be focused on economic advantage (through attacks like intellectual property theft, personally identifiable information theft, or other thefts of other economic advantage). Their motives are primarily geared towards positioning themselves in the best possible situation geopolitically. This could be as simple as providing more competitive advantage economically to their corporations, spying on our national intelligence apparatus, or it could be as multilayered as providing deep intrusions into the US critical infrastructure in preparation for a 'cyber response' to a 'kinetic action'.

To that last point, public officials, such as the Five Eyes (an intelligence sharing alliance including Australia, Canada, New Zealand, the United Kingdom, and the United States, with cybersecurity being a key area for cooperation, including sharing information and coordinating efforts to counter cyber threats) and Chris Krebs, have warned the public about the threat China poses to critical infrastructure. Chris Krebs was CISA's Director under the first Trump Administration and is considered a well-trusted advocate for US defensibility. In a *Wall Street Journal* podcast conducted in October of 2024, he stated that "President Xi has directed his military to be ready for a takeover of Taiwan by 2027", "...they are outstripping us [in cyber] by 600,000 cyber offensive operators" and "... the most concerning thing is they've [China] also directed their military to start pre-positioning in critical infrastructure[3]. This effectively means establishing a logistical foothold in US critical infrastructure, which is inclusive of healthcare, and preparing for large scale cyberwarfare to cause disruption to our critical infrastructure in response to a kinetic military action against them.

In healthcare, this is a substantial problem. Though we have forums to provide collaborations and defense, such as the HSCC CWG or the Health Information Sharing and Analysis Center (Health-ISAC), our critical infrastructure operators are run by private companies. Within healthcare delivery, such as hospitals and clinics, this tends to be not-for-profit organizations with razor thin margins. (Fitch projects a median margin of between 1% and 2% in 2025[4].) Expecting such organizations to have the financial and technical resources to defend on their own against a nation state is unrealistic.

[3] Cybersecurity Expert Chris Krebs Warns of Risks to US - The Wall Street Journal Google Your News Update - WSJ Podcasts

[4] https://www.hfma.org/finance-and-business-strategy/hospital-financials-are-projected-to-continue-trending-upward-this-year/

The methods deployed to conduct such attacks are varied, but the theme is generally the same: it's tenacious, specific, targeted, and strategic. We see the following methods deployed:

1. Deep supply chain attacks, whereby infiltration happens at the software component level during development, or allegedly establishing hardware backdoors directly into hardware when manufactured.
2. Sophisticated hacking from the Chinese arsenal, such as Volt Typhoon's targeting of the water critical infrastructure, as described by General Timothy Haugh in an April 2024 NY Times article[5]. Specifically, he stated "China was securing access to critical networks ahead of a direct confrontation between the two countries".

The implications of these kinds of threats are real and potentially incredibly damaging.

Organized Crime

Though sometimes confused with Nation State Actors, organized crime has entered the global stage with a different context. Primarily fiscally motivated, these threat actors tend to break in fast and cause as much prolonged damaged as possible, without being surgical, tactical, or targeted. Generally, this tends to be an attack of opportunity – the victim happens to be in the wrong place, with the wrong defenses, at the wrong time. The goal is always the same: cause as much damage for as long as possible in order to force the victim to pay for an extortion. It's the bank heist of the 21st century.

These attacks are the attacks you read about often in the news. The Russian speaking criminal organization ALPHV/BlackCat took down Change Healthcare and disrupted the healthcare claims and

[5] China Could Threaten Critical Infrastructure in a Conflict, N.S.A. Chief Says - The New York Times

payments ecosystem[6]. The Russian speaking criminal organization DarkSide shut down the Colonial Pipeline.[7]

The methods deployed by these types of organized crime and ransomware operators tend to be consistent. Their sophistication comes from running their cyber operations at scale, leveraging common vulnerabilities, across multiple industries to find compelling targets susceptible to attack, and likely willing to pay for an extortion. The methods they use are largely based around a failure of these organizations to deploy proper controls and maintain cyber hygiene. A failure of cyber hygiene is not necessarily a result of a lack of due diligence, but rather a reflection of the fluidity of the digital ecosystem that continually changes to meet our healthcare needs. Defense involves constant, continual, and evolving rigor. The scale of the digital ecosystem of any organization can easily run from tens to hundreds of thousands of connected devices.

As we studied with the Landscape Analysis, the methods for initial entry tend to fall into three categories:

1. Social engineering, through attacks such as phishing, but also impersonation attacks to service desks, multifactor authentication fatigue attacks, and credential spraying (where credentials from other third-party breaches are reused).
2. Remote code execution vulnerabilities that are exposed directly to the Internet, that are not patched, and are actively being exploited by bad actors (such as the Known Exploited Vulnerabilities (KEVs) posted by CISA[8]). Importantly, while there are millions of vulnerabilities that have been discovered, CISA posts only the actively exploited vulnerabilities which are

[6] How the ransomware attack at Change Healthcare went down: A timeline | TechCrunch
[7] The DarkSide Hacker Group: Who and What Are They
[8] Known Exploited Vulnerabilities Catalog | CISA

currently tracking at 1310 KEVs. The goal is not to get to zero vulnerabilities, but to patch the KEVs and other highly exploited vulnerabilities first.

3. A third-party who is connected to your organization through a risky network connection, such as a permanent VPN, a remote access system without multifactor authentication or control, or other 'side channel' access.

Though these three methods are the primary methods used to get access to corporate networks this is not the end of the attack. Once inside the target is ultimately the IT administrators and control over systems that run the digital ecosystem in which the health system resides. They subvert the access that these IT administrators have, after moving laterally in the environment, and then take the same control the IT administrator has to cause the most damage possible. It's a "nuclear option" style attack because rebuilding the entire digital ecosystem is a daunting task that takes on average between 20 to 180 days.

Current State of Medical Device Security Defenses

The primary concerns with attacks against medical devices are related to patient safety and national security. Additionally, they can be used for conduits for further attack against an organization. Though there have been no known public attacks against medical devices to cause harm to a patient, the studies and research have shown that such an attack is possible. One such study in 2011 showed how it was possible to compromise an insulin pump to deliver fatal dosages of medications, though it has never been reported to have happened.[9]

[9] Insulin pump hack delivers fatal dosage over the air • The Register

These types of attacks have caused the healthcare industry, the US Department of Health and Human Services, and the Food and Drug Administration (FDA) to establish numerous task groups under the HSCC CWG to tackle these challenges. I'd like to highlight a few of those successes over the last 8 years.

1. The Industry/DHHS Joint Publication 405d Landscape Analysis Task Group emphasized that network-connected medical devices, such as imaging, pharmacy, and laboratory equipment, are particularly vulnerable to cyber threat.
2. The Industry/DHSS Joint Publication 405d Health Industry Cybersecurity Practices (HICP) established an entire practice for hospitals and healthcare providers for deploying and securing medical devices, emphasizing their unique nuances for quality control and management, specifically outlining network security, risk management, asset management, patching, and incident management practices for medical technology.
3. The Industry, with participation from the FDA, released the Joint Security Plan which outlined methods that Medical Device Manufacturers (MDMs) could follow to build security in by default and design[10]
4. A medical technology vulnerability management toolkit, which describes the best way for MDMs to communicate to their customers key vulnerabilities for their technologies[11]
5. A comprehensive guide for managing medical technology, named HIC-MaLTS.[12]

[10] https://healthsectorcouncil.org/jsp2/

[11] https://healthsectorcouncil.org/medtechvulncomms/

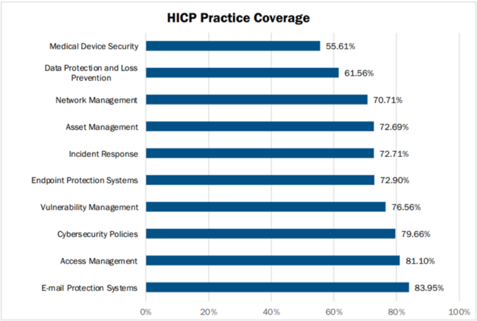
[12] https://healthsectorcouncil.org/legacy-tech-security/

6. A collaboratively written industry guide with pre-defined contractual language that can be used between MDMs and health delivery organizations (HDOs), called the Model Contract Language for Medtech Cybersecurity.[13]

This represents the great work that the industry and the US Government have completed since 2018 working together as collaborative partners. We have defined "what" needs to happen, however the actual implementation of these practices has been varied.

The Landscape Analysis showed that on average, hospitals only have about 55% of the HICP-recommended practices for medical device security implemented. Medical device security, as shown below, is the least protected amongst the hundreds of health systems analyzed. Work can be done by HDOs to improve their medical device defenses.

Figure 11 HICP average percent coverage by practice



The challenge for providing cybersecurity coverage for these devices, in practice, actually relates to the intrinsic nature and purpose of the devices themselves. These devices are diagnostic or therapeutic by design. The quality of the data produced by the devices for diagnostic purposes, or the therapies that

[13] https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2/

they deploy, are paramount for patient safety. Additionally, these devices run on technology, which is fallible by its nature. Without proper quality control, in our zeal to fix a cybersecurity vulnerability we can cause more harm than good. Further complicating all of this is the fact that steps to protect medical device security can cause disruption or outages to systems that were never designed to be patched as general IT systems are patched, or worse yet, cause harm to patients because of haphazard approaches. In some cases, it's not even possible for the HDOs themselves to be one the ones to deploy patches but rather it must be the MDMs themselves, given the sophisticated and highly specialized nature of the technology. As such, the process is slower for safely managing the life cycle of these devices, for reasons that are reasonable and understandable.

Collective Defense

We must do better. All parties agree to this construct and appreciate the complexity of the challenge. Though it might be easy to point a finger and say, "It's the HDOs' fault for failing to deploy good cyber hygiene", or "It's the MDMs' fault for having flawed security by design", or "It's the FDA's fault for not regulating this industry more strictly", none of these statements respect or reflect the totality and immensity of the challenge.

We need a comprehensive approach to this problem that includes the private sector and government.

1. Re-establish the Critical Infrastructure Policy Advisory Committee (CIPAC), or some construct of similar protection and ability, so that the healthcare industry and the Federal Government can once again establish an open dialogue to discuss these vulnerabilities without fear of industry specific vulnerabilities being made public through activities such as Freedom of Information, public forums, or other outlets. CIPAC provided the forum through which all Critical Infrastructure owners and operators partnered with their Sector Risk Management Agency

(SRMA). A recent Executive Order disrupted that partnership. On March 13th the Department of Homeland Security provided notice via the *Federal Register* that CIPAC would no longer be effective as of March 7th, 2025[14].

2. Continue to expand the Federal Government partnership with the healthcare industry by leveraging the Private Sector Clearance Program for Critical Infrastructure.[15] Within this program there should be more CISOs of key critical infrastructure organizations cleared for classified information sharing.
3. Once clearances have been established, establish a regular and recurring threat briefing amongst national intelligence agencies, SRMAs, and key critical infrastructure operators across all critical infrastructure. The purpose of these briefings should be focused on getting key actions into the hands of the critical infrastructure operators, without attribution of sources, so that we can provide a strong signal of response to national threats. Today such a program does not exist outside of the Cybersecurity & Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) Flash Reports that are difficult to consume for resource strapped healthcare entities.
4. Federal encouragement of membership in the HSCC CWG. Our collective defense depends on all critical infrastructure operators working together. Today, the HSCC CWG includes 450 organizations that make up critical infrastructure within the healthcare industry, however there are thousands of operators in this space. Dues are not permitted, under CIPAC, and any member of the health sector can join. The web address to join is https://healthsectorcouncil.org.
5. Reauthorize the Cybersecurity Act of 2015, which created Section 405(d) and ultimately accounted for the creation of HICP. Public Law 116-321, signed by President Trump on January

[14] Federal Register :: Notice of Termination of Discretionary Federal Advisory Committees.

[15] DHS/CISA/PIA-020 State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure | Homeland Security

5th 2021, specifically identified the 405(d) products as "recognized security practices" and instructed the HHS Office for Civil Rights (OCR) to consider the adoption of HICP practices over a period of 12 months during enforcement actions. This has been largely lauded as a great 'carrot' towards getting investment and making collective improvements without overly punitive regulations that are not geared towards directly managing the threats we face. Unfortunately, the proposed modifications to the HIPAA Security Rule that were released on December 27, 2024 by OCR conflict with this law[16].

6. Establish a Joint Task Force to study the specific problem related to nation state actors attacking and compromising medical technology. Unfortunately, it's largely unknown how systemic and material this problem is. The Task Force could be made up of Critical Infrastructure operators, MDMs, academics, our national intelligence apparatus, and key cybersecurity specialists who track and monitor nation state actions. This Task Force's deliberations and products could be classified to preserve the integrity and free sharing of information with the sole purpose of building a better collective defense.
7. Amplify the great work already released under the HSCC CWG, the FDA and Health-ISAC that has focused tirelessly on bringing best practices into the industry. Credibility by amplification through the highest levels of Government will help provide the focus executives need to dedicate time and resources to these challenges.

[16] https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information

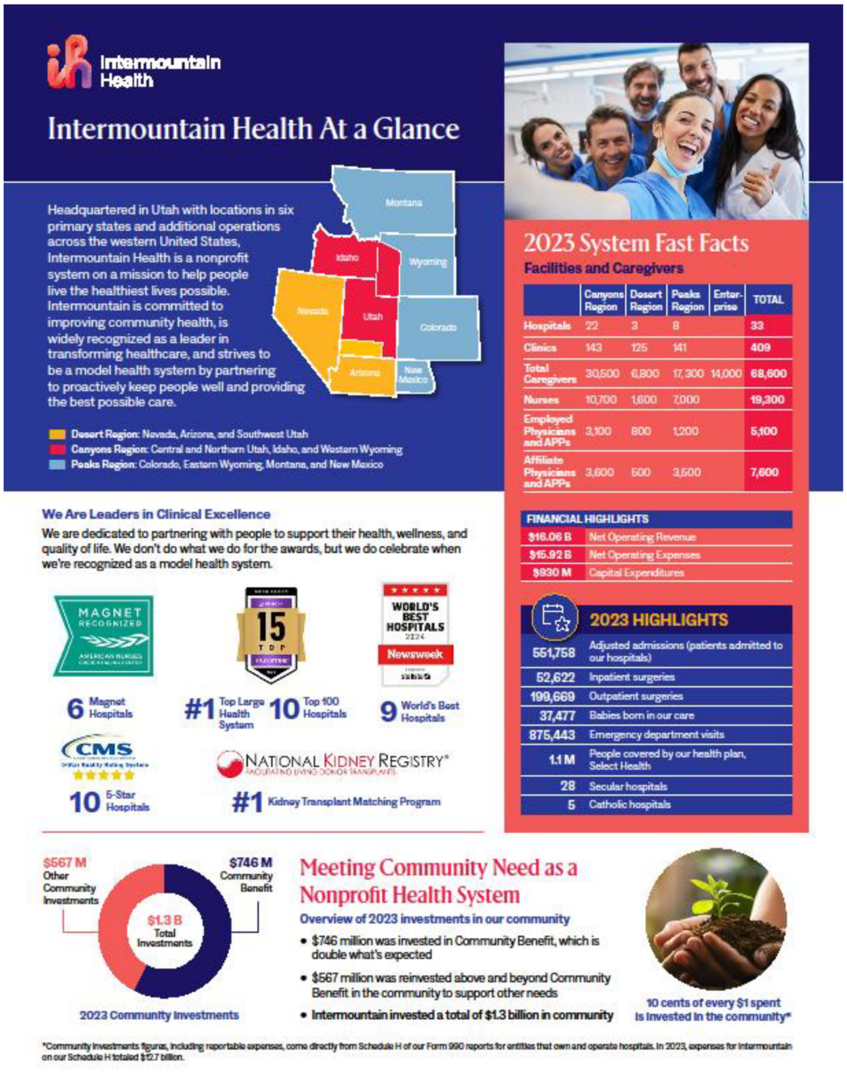
Strengthening the Bonds of the Future

Imagine a future where a single threat signal permeates the whole of all 16 critical infrastructure sectors, with a tight package of mitigating responses and a coordinated and cohesive counter to the threat. Like our bodies which have built a complicated immune system to respond to threats in such a manner, similar defenses can be created for cybersecurity resilience in healthcare. In large part these defenses are fully preventative; we do not get sick when encountering every pathogen in our environment. In other cases, our defenses are highly reactive and responsive. We might fall ill for a few days when managing the common cold, but we do recover and then imprint that defense into our immunity. With the right protective measures and working together we can improve our collective cyber posture such that our ability to respond to cyber events is stronger.

Thank you for the opportunity to provide testimony at this hearing. Hopefully I have convinced you that cybersecurity challenges are not technology challenges alone, but in fact require strategies, programs, policies, and partnerships to effectively protect our nation's health and security. We must embed cybersecurity into the very fabric of all 16 critical infrastructure sectors, and most importantly the HPH and Government sectors. The ability to defend and respond to attacks is critical to protecting human life and safety. We hope you will agree that: cyber safety is atient safety, and cybersecurity is national security.

In closing, I would like to echo the words of our previous National Cyber Director, Chris Inglis. We must set up our nation's Critical Infrastructure in such a way that "**you must beat all of us to beat one of us**". I look forward to working together to realize that vision.

Intermountain Facts and Figures



Intermountain Health
Montana
Idaho
Wyoming
Nevada
Utah
Colorado
Arizona
New Mexico
MAGNET RECOGNIZED
AMERICAN NURSES
15 TOP
WORLD'S BEST HOSPITALS 2024
Newsweek
CMS
NATIONAL KIDNEY REGISTRY®
FACILITATING LIVING DONOR TRANSPLANTS

Intermountain Health At a Glance

Headquartered in Utah with locations in six primary states and additional operations across the western United States, Intermountain Health is a nonprofit system on a mission to help people live the healthiest lives possible. Intermountain is committed to improving community health, is widely recognized as a leader in transforming healthcare, and strives to be a model health system by partnering to proactively keep people well and providing the best possible care.

- 🟧 **Desert Region:** Nevada, Arizona, and Southwest Utah
- 🟥 **Canyons Region:** Central and Northern Utah, Idaho, and Western Wyoming
- 🟦 **Peaks Region:** Colorado, Eastern Wyoming, Montana, and New Mexico

2023 System Fast Facts

Facilities and Caregivers

	Canyons Region	Desert Region	Peaks Region	Enter-prise	TOTAL
Hospitals	22	3	8		33
Clinics	143	126	141		409
Total Caregivers	30,500	6,800	17,300	14,000	68,600
Nurses	10,700	1,600	7,000		19,300
Employed Physicians and APPs	3,100	800	1,200		5,100
Affiliate Physicians and APPs	3,600	500	3,500		7,600

FINANCIAL HIGHLIGHTS	
$16.06 B	Net Operating Revenue
$15.92 B	Net Operating Expenses
$930 M	Capital Expenditures

2023 HIGHLIGHTS	
551,758	Adjusted admissions (patients admitted to our hospitals)
52,622	Inpatient surgeries
199,669	Outpatient surgeries
37,477	Babies born in our care
875,443	Emergency department visits
1.1 M	People covered by our health plan, Select Health
28	Secular hospitals
5	Catholic hospitals

We Are Leaders in Clinical Excellence

We are dedicated to partnering with people to support their health, wellness, and quality of life. We don't do what we do for the awards, but we do celebrate when we're recognized as a model health system.

6 Magnet Hospitals

#1 Top Large Health System **10** Top 100 Hospitals

9 World's Best Hospitals

10 5-Star Hospitals

#1 Kidney Transplant Matching Program

2023 Community Investments

Meeting Community Need as a Nonprofit Health System

Overview of 2023 investments in our community

- $746 million was invested in Community Benefit, which is double what's expected
- $567 million was reinvested above and beyond Community Benefit in the community to support other needs
- **Intermountain invested a total of $1.3 billion in community**

10 cents of every $1 spent is invested in the community*

*Community investments figures, including reportable expenses, come directly from Schedule H of our Form 990 reports for entities that own and operate hospitals. In 2023, expenses for Intermountain on our Schedule H totaled $12.7 billion.

Mr. BALDERSON. Thank you, Mr. Decker.

Ms. Jump, 5 minutes.

STATEMENT 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 premarket 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 healthcare 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:]

Testimony of

Michelle Jump
Chief Executive Officer

of

MedSec LLC

on

Aging Technology, Emerging Threats:
Examining Cybersecurity Vulnerabilities in Legacy Medical Devices

Before the

United States House of Representatives

Committee on Energy and Commerce

Oversight and Investigations Subcommittee

April 1, 2025

Introduction

Chairman Palmer, Ranking Member Clarke, and members of the Committee, my name is Michelle Jump. I am the Chief Executive Officer of MedSec, a consulting and technical services firm focused on medical device and healthcare cybersecurity.

I appear before you today to share my perspective as someone who has spent the past 15 years helping organizations understand and navigate the introduction of emerging technologies in the medical device industry. Over that time, I have witnessed the industry move from initial recognition to full embrace of the promise that connected technologies bring—not only in making healthcare delivery faster, more efficient, and more accurate, but also in recognizing the new risks these innovations introduce.

As we connect more medical devices across hospitals, homes, and care centers, we also expose those systems to new threats. One such unexpected and significant threat is to the cybersecurity of our critical healthcare infrastructure.

As a regulatory and quality expert—not a technical one—my focus has not been on how to integrate or defend these technologies, but on understanding how innovation can unintentionally introduce risk even as it aims to provide solutions. This is the tradeoff we must manage in exchange for the benefits of connected technology.

Throughout my career, I have served as an active member and leader in numerous industry working groups, standards committees (both domestic and international), and trade associations. My life's work has been dedicated to ensuring that these critical technologies can be safely and securely integrated into the healthcare system—delivering on their promise to support clinicians in providing the highest quality patient care.

We appreciate the Committee convening this timely hearing to examine cybersecurity in the health sector, particularly as it relates to medical technology. Today, my testimony will focus on how cybersecurity in the medical device industry is currently regulated, and how we—as a collective of stakeholders—can work together to make the adoption of emerging technologies safer and more secure for the patients and healthcare providers who rely on them.

Today, I will cover seven areas of consideration on this topic:

First, a brief overview of how the increased utilization of connected technology in the health sector increases cyber risk;

Second, a review of the regulatory expectations for cybersecurity in medical devices and how the industry has responded to increasing cybersecurity expectations;

Third, a discussion of the cybersecurity challenges of the healthcare delivery organizations (e.g. hospitals);

Fourth, an explanation of the risk transfer process where the risk management of legacy medical devices moves from the medical device manufacturer (MDM) to the healthcare delivery organization (HDO);

Fifth, a review of how the health sector is targeted for cyber attacks;

Sixth, a description of the need to address the gap in qualified and trained cybersecurity professionals to support the health sector; and

Seventh, a summary of recommended actions to aid in the reduction of risk to the health sector from cybersecurity threats, subdivided into categories of Industry-wide, MDM, HDO, Suppliers, and Regulators.

About MedSec

As a global leader in medical device product security, MedSec drives industry wide improvements to the practice of medical device and healthcare security by providing a comprehensive range of cybersecurity services—including regulatory consulting, program and process development, workforce training, and technical services such as penetration testing and threat modeling. While MedSec is a smaller, boutique firm, when considering the combined revenue of our clients, we represent over 70% of the global medical device industry, by serving the full spectrum of medical device manufacturers from global corporations to start-ups.

In addition to its work with medical device manufacturers, MedSec is also deeply engaged in strengthening cybersecurity across the broader healthcare ecosystem through the participation in working groups, standards, and conferences. We partner closely with clients to help address their most pressing cybersecurity challenges, improve organizational resilience, and build long-term capacity for managing risk in an increasingly connected healthcare environment.

How Digital Integration Has Increased Cyber Risk in Healthcare

Over the past few decades, the healthcare environment has transformed significantly. What was once a largely paper-based system with standalone medical devices has evolved into a highly interconnected ecosystem. Today's healthcare relies heavily on modern, networked medical device systems that share and depend on digitally stored data. Paper charts have been replaced by electronic health records (EHRs), and medical devices are increasingly software-driven. The once-clear boundaries between devices, systems, and data flows are rapidly disappearing.

As a result, healthcare delivery has adapted to embrace this new level of integration. EHRs are now the standard, and medical devices routinely transmit information across the care environment. These components work together in real time to support clinical workflows. For example:

- Medical devices located in patient rooms or at the bedside now communicate directly with central nursing stations. This allows fewer staff to safely monitor more patients.
- Devices are increasingly designed to transmit data directly into EHR systems, reducing staff workload. Some are even beginning to receive data from EHRs to preconfigure settings and improve workflow efficiency.
- Diagnostic imaging devices send images to radiologists for faster review, eliminating the need for on-site interpretation. Both images and results can be uploaded directly to the EHR.
- Implanted and wearable devices now connect to patients' smartphones to monitor performance and treatment. These devices also transmit data to clinicians, enabling timely follow-ups or urgent interventions when needed.

These are just a few examples of how healthcare technology has evolved—and how deeply dependent it has become on connectivity. A cybersecurity incident can significantly disrupt this interconnected environment. For example, a ransomware attack that disables hospital networks—or leads to systems being shut down as a precaution—can force immediate, resource-intensive changes to clinical workflows and staffing.

Hospitals may need to:

- Increase the number of nurses to manually monitor patients at the bedside
- Manually enter data into EHRs or revert to paper-based documentation, a time-consuming process
- Require radiologists to interpret images on-site or manually transfer imaging files
- Conduct in-person follow-ups for patients with implanted or wearable devices due to lost remote monitoring capabilities

In addition, if one facility is compromised and must divert patients, surrounding hospitals must be prepared to accommodate unexpected surges in patient volume.

Medical Devices

Medical devices have undergone significant transformation over the past several decades, incorporating new technologies to better serve both patients and healthcare providers. Historically, these devices were primarily hardware-based. Over time, however, they evolved to include software, connectivity to networked infrastructure and electronic health records (EHRs), and integration with commercial technologies such as Bluetooth and cloud service providers. This shift has significantly expanded the risk landscape for medical devices, particularly in terms of cybersecurity.

For over a decade, the FDA has been steadily raising the bar on cybersecurity expectations as part of its regulatory oversight. The agency released its first final premarket cybersecurity guidance in 2014[1], followed by postmarket cybersecurity guidance in 2016[2]. These documents emphasized that cybersecurity is a shared responsibility across the healthcare sector and urged manufacturers to consider security early in the design process as well as throughout postmarket device management.

While progress was being made under this framework, the rising frequency of ransomware attacks on hospitals, and increasing instances of medical devices being affected, led the FDA to call for explicit cybersecurity authority in its 2018 Medical Device Safety Action Plan[3].

A significant advancement came with the enactment of the Food and Drug Omnibus Reform Act (FDORA)[4], which granted the FDA new authority through the addition of Section 524B to the Food, Drug, and Cosmetic Act and went into effect on March 29, 2023. This provision establishes explicit cybersecurity requirements for medical devices undergoing marketing authorization. In parallel, the FDA issued updated premarket cybersecurity guidance

[1] U.S. Food and Drug Administration (FDA). (2014). *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (Guidance for Industry and Food and Drug Administration Staff). Center for Devices and Radiological Health. October 2, 2014

[2] U.S. Food and Drug Administration (FDA). (2016). *Postmarket Management of Cybersecurity in Medical Devices* (Guidance for Industry and Food and Drug Administration Staff). Center for Devices and Radiological Health. December 28, 2016

[3] U.S. Food and Drug Administration (FDA). (2018). *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health.* Center for Devices and Radiological Health. April 2018

[4] U.S. Congress. (2022). *Food and Drug Omnibus Reform Act of 2022*, Division F of the *Consolidated Appropriations Act, 2023*, Pub. L. No. 117-328, 136 Stat. 4459, 5689–5740 (Dec. 29, 2022)

entitled Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions[5].

FDA's implementation of these new legislative authorities and FDA Guidance has balanced the needs of patients by continuing to authorize innovative technologies while also holding manufacturers accountable for devices that simply carry too many cybersecurity risks.

These strengthened authorities and clearer expectations have already begun to drive meaningful changes across the medical device industry. Although often prompted by regulatory pressure during the submission process, manufacturers are increasingly shifting their mindset. Where once there was a willingness to "take their chances" with minimal cybersecurity integration, many now proactively ask, "What do we need to do?"

Some manufacturers have already been adapting, making substantial internal changes to embed cybersecurity into their organizational culture and business practices. However, lasting impact depends on continued leadership support, as such changes take time to fully mature and become part of the lasting culture within the organization.

Importantly, these cybersecurity expectations apply not only to new devices but also to existing devices undergoing modifications that require resubmission to the FDA.

The FDA has started to implement and, in some instances, require submissions to be provided to the Agency with their electronic submission template (eSTAR). This template is

[5] U.S. Food and Drug Administration (FDA). (2023). *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions* (Final Guidance). Center for Devices and Radiological Health. September 27, 2023

dynamic and based on how information is entered, can enforce sections to be completed and that documentation is attached and/or certain questions are answered to allow the submission to proceed. If a manufacturer is missing information, the manufacturer cannot submit their application. The eSTAR barrier to submission entry is an important deterrent to "throw documents at the wall and see what FDA reacts to." It raises the general incentive to provide solid documentation from the start so that they do not delay the start of their submission process. All products going through submission due to modification, regardless of whether that modification is related to cyber, must meet the current cybersecurity "bar" set by the FDA. Companies respond to this.

As medical device manufacturers continue to mature their cybersecurity programs and strengthen the protections within their products, market pressure is also playing a growing role. Hospitals and healthcare systems are placing greater importance on cybersecurity when making purchasing decisions. Increasingly, strong security features are seen as a market differentiator, while poor or absent security can be a dealbreaker. Hospitals can further drive this trend by establishing and consistently enforcing robust cybersecurity requirements in their procurement processes.

Healthcare Delivery Organizations

Cybersecurity practices at the hospital, including a commitment to maintaining secure devices, and the environment medical devices operate in are equally important. Maintaining a secure environment for hospital networks is a shared responsibility between healthcare delivery organizations (hospitals), health IT companies/EHR vendors, makers of operating systems and other software infrastructure, end users, and medical device manufacturers.

Healthcare Delivery Organizations (HDOs) have faced similar technological evolutions as medical devices have depended on more connectivity and advanced technology. The healthcare environment has become increasingly interconnected between medical devices, electronic health records, their networks, billing systems, pharmaceutical order systems, Laboratory Information Systems, imaging systems, and cloud environments. As discussed earlier, cybersecurity incidents in this connected environment can significantly impact delivery and timeliness of clinical care unless additional, qualified personnel are available to staff the disconnected workflow. They also have general operational environment cybersecurity risks from connected elevators, HVAC systems, hosting Wi-Fi networks, etc.

The rapid adoption of connectivity within HDOs has, in many cases, outpaced comprehensive cybersecurity planning. As a result, many healthcare facilities have not yet fully assessed or addressed all vulnerabilities in their connected environments. In recent years, however, there has been an increased focus on strategies such as network segmentation, which can help limit the impact of cyber incidents and improve the overall security posture of healthcare systems.

Risk Transfer: The Path to Legacy

As medical devices age and can no longer be effectively secured against modern cybersecurity threats, they enter a lifecycle stage known as End of Support (EOS). At this point, the device's manufacturer or software providers cease offering updates, security patches, and technical assistance. This typically occurs when key components—such as the operating system—are no longer supported, or when the underlying technology becomes obsolete and cannot be reasonably upgraded or maintained.

If a Healthcare Delivery Organization (HDO) chooses to continue using the device beyond this point, there are no current regulations that prohibit doing so. However, the responsibility for managing the cybersecurity risk associated with continued use of that device is transferred from the manufacturer to the HDO. This transition of responsibility is known as risk transfer.

Risk transfer is not a passive event, it is a formal process that requires deliberate actions and informed decision-making. Continued safe use of legacy medical devices depends on the HDO's ability to assess, document, and manage the security risks introduced by the device. This includes implementing compensating controls, conducting regular risk assessments, monitoring device behavior, and isolating the device from other networked systems where necessary.

This process has been well-documented in industry guidance, including the *Health Sector Coordinating Council's (HSCC) Health Industry Cybersecurity - Managing Legacy Technology Security (HIC-MaLTS*) and the International Medical Device Regulators Forum (IMDRF) guidance *Principles and Practices for the Cybersecurity of Legacy Medical Devices*[6]. These documents offer frameworks for risk management when legacy systems remain in use, outlining the actions HDOs should take to minimize potential harm to patients and disruption to clinical workflows.

However, the effectiveness of risk transfer relies heavily on the maturity of the HDO's internal processes and the availability of appropriately trained personnel. Not all healthcare organizations are equally equipped to take on this added responsibility. In particular, small, rural, or resource-constrained hospitals may lack the cybersecurity staff, asset inventory systems, or governance structures needed to safely manage legacy device risks.

This growing challenge highlights the need for:

- Standardized processes for managing EOS medical devices across HDOs;
- Investment in workforce development, including training for clinical engineering and cybersecurity personnel responsible for legacy device oversight; and
- Improved collaboration between manufacturers and HDOs to ensure transparency around device support lifecycles and to enable proactive planning for EOS transitions.

As healthcare technology continues to evolve rapidly, the accumulation of unsupported legacy devices within hospital environments presents a serious long-term risk. Without adequate processes in place to manage risk transfer, patient safety and operational continuity may be compromised. There is an opportunity for regulatory bodies, industry stakeholders, and healthcare providers to work together to develop more robust mechanisms for handling legacy device risk, ensuring that continued use of older technology does not come at the cost of cybersecurity or clinical effectiveness.

Who's the Target?

Medical device cybersecurity is frequently covered in the media and is often a focal point in discussions about the broader cybersecurity posture of the healthcare sector. A history of notable gaps in cybersecurity controls, along with high-profile reports highlighting serious vulnerabilities, has drawn scrutiny to medical devices in general as potential threats to critical healthcare infrastructure.

However, while medical devices attract significant attention, the most common and impactful cybersecurity threat facing hospitals—**ransomware**—rarely originates from the devices themselves. Typically, ransomware is designed to be introduced into hospital networks through human error, such as an employee clicking on a malicious link in a phishing email. Once inside the network, the malware can spread laterally. If medical devices are not adequately secured or segmented, they too can become infected or disrupted, compounding the impact of the attack.

This raises an important question: Does this mean that medical device security is less important? The answer is unequivocally no. Instead, it highlights the complexity of the issue and the extent to which cybersecurity must be treated as a shared responsibility. The security of a medical device when it leaves the manufacturer, right out of the box, is just one piece of a much larger puzzle. The cybersecurity practices of the Healthcare Delivery Organization (HDO), including how they maintain, configure, and manage medical devices within their operating environment, are equally critical to overall system security. Additionally, insecure medical devices can serve as entry points into the hospital, particularly those connectable to external systems.

Manufacturers can and should continue to be held to high standards for building secure devices, standards reinforced by recent legislative and regulatory changes such as Section 524B of the Food, Drug, and Cosmetic Act. However, even the most secure device can be exploited if it is placed into an unprotected or under-resourced environment. Hospitals, especially those with limited funding, often lack the financial and personnel resources to replace aging equipment or maintain sophisticated cybersecurity programs. As a result, legacy devices—known to have vulnerabilities—remain in active use not because of negligence, but due to a lack of alternatives.

Thus, ensuring that hospitals have access to secure technologies and that manufacturers maintain and update device security throughout the product lifecycle is essential but not sufficient on its own. Medical Device Manufacturers (MDMs) play a crucial role, but systemic underinvestment in cybersecurity at certain hospitals, particularly smaller or rural hospitals, remains a significant barrier to meaningful risk reduction.

Addressing this challenge requires a coordinated approach that includes:

- Supporting HDOs in building secure digital environments,
- Providing technical and financial assistance to enable device upgrades and secure network architectures,
- Ensuring manufacturers maintain security support throughout a product's lifecycle, and
- Continuing to reinforce the shared nature of responsibility between manufacturers, hospitals, and the broader healthcare system.

Ultimately, medical device cybersecurity cannot be effectively addressed in isolation. It must be part of a holistic strategy that recognizes the interdependence between devices, healthcare infrastructure, and the broader threat landscape. Regulatory guidance, targeted funding, and strong cross-sector collaboration will all be essential in helping hospitals keep pace with evolving cyber threats and protecting patient safety.

Missing Voice

Medical devices increasingly rely on commercial technologies such as Windows operating systems, Bluetooth connectivity, commercial and open-source software, and off-the-shelf chipsets. The integration of these components helps drive down development and production costs, ultimately contributing to efforts to contain rising healthcare expenses.

However, the security of these commercial components is directly tied to the security of the medical devices that incorporate them. Despite this critical connection, there remains insufficient focus on securing these foundational technologies. Compounding the issue, medical devices often rely on commercial software and hardware well beyond the lifecycle originally intended by the developers or vendors of these general use components.

This is where Software Bills of Materials (SBOMs) play a critical role. SBOMs provide visibility into the third-party and open-source components used in a medical device, helping manufacturers, regulators, and healthcare providers understand what software is present and what associated vulnerabilities may exist. Without SBOMs, it becomes significantly more difficult to assess risk, manage vulnerabilities, or respond quickly to newly discovered threats within a device's software supply chain.

Without involving these upstream technology providers in ongoing discussions—and without encouraging longer support lifecycles—we will continue to face systemic vulnerabilities in medical devices. Ensuring that these foundational technologies are developed and maintained with security and longevity in mind is essential to improving the overall resilience of healthcare technology.

This is also a People and Process Issue

The healthcare industry faces a critical shortage of trained cybersecurity professionals with the expertise required to manage security in a dedicated and strategic way. This is fundamentally a **people and process issue**. Without skilled personnel on the ground to guide secure practices, manage risk effectively, and accurately assess and monitor what is connected to hospital networks, we are at a severe disadvantage.

This is not something that can be addressed through regulation alone. The FDA, while instrumental in setting important standards and expectations, cannot regulate its way into better on-the-ground cybersecurity management. What's needed is a workforce that understands the unique complexities of healthcare environments and is capable of making informed, real-time decisions to protect patients and systems.

At present, we simply do not have enough qualified cybersecurity professionals to meet the growing demands of the sector. In my view, this talent shortage is a core issue. Without experienced cybersecurity staff embedded in healthcare settings—individuals who can identify vulnerable legacy devices, advocate for more secure infrastructure, and drive change from within—unsafe practices will persist and hospitals will remain vulnerable.

What makes this issue even more urgent is the **imbalance between supply and demand**. When skilled cybersecurity professionals are scarce and the competition for talent is high, many hospitals—particularly small or rural facilities—are priced out. They often cannot afford to hire or retain qualified staff, and as a result, go without. This workforce gap leaves many organizations unprepared and under-defended.

It is essential that this issue receives more focused attention. Workforce development, training incentives, and targeted funding to build internal cybersecurity capacity must be prioritized if we are to meaningfully improve the security posture of the healthcare sector.

Solutions – How Can We Address This

Meaningful progress in securing legacy medical devices requires a coordinated and sustained effort from both medical device manufacturers (MDMs) and Healthcare Delivery Organizations (HDOs). This is not solely a technological challenge—it is fundamentally a people and process issue. Even the most secure medical device, if deployed without proper ongoing support and oversight, can become vulnerable over time. Many connected medical devices are used far beyond their intended useful life, even for 20 years or more, making long-term security a critical concern. Security is not a “one-and-done” feature, it requires continuous attention, including staff training, well-defined processes, and routine maintenance. Without trained personnel at both MDMs and HDOs who understand and follow established cybersecurity practices, the legacy device problem will persist. Likewise, without a shared commitment from both parties to develop and apply updates, manage device configurations, and maintain the overall cybersecurity posture of devices and hospital networks, the risk associated with legacy technologies will continue to grow.

Currently, one of the most comprehensive resources available for addressing this issue is the Health Sector Coordinating Council (HSCC) *Health Industry Cybersecurity - Managing Legacy Technology Security*, (HIC-MaLTS). This document outlines best practices for managing legacy medical devices and provides practical, actionable guidance. However, it is important to note that this report is voluntary. It is a best practice guide, not a regulatory or enforceable policy document from agencies such as the FDA, CMS, or The Joint Commission.

To drive meaningful change, there must be greater alignment between voluntary best practices and enforceable expectations, as well as increased investment in training, process development, and long-term cybersecurity planning by both MDMs and HDOs.

Recommendations

Industry-Wide

1. More trained security people with the experience to manage security in a dedicated way. This can come in the form of focused development of staff already in place by supplemental training and development or in the investment of regional and virtual training programs to develop an expanded security-savvy workforce.
2. Focus on effective communication programs to help HDOs and MDMs better communicate and coordinate their shared responsibilities in maintaining health sector security.

Medical Device Manufacturers

1. Develop more security engineers who can help design more secure devices from the outset, aiding in the delay of entering a legacy state.
2. Mature communication with stakeholders regarding the support status of marketed devices. Customers should be notified in advance of a product going EOS and this should typically occur when necessary due to the MDM's inability to support the product.
3. Practice good supply chain management. Review the software components chosen to be added to a medical device and select those more effective at maintaining the device for a reasonable time once launched into the market.
4. Develop, commit to, and execute regular software maintenance activities to patch vulnerabilities as they occur, as is now required by Section 524B for devices going through premarket submissions reviews. Do not allow vulnerabilities to build up over time and increase the "defect density" simply because that vulnerability is lower risk on its own. Vulnerabilities can be chained together to create a larger impact attack. Default activities should be to patch newly identified vulnerabilities rather than leave them in place.
5. For current legacy medical devices, MDMs can evaluate how much cybersecurity risk they can manage while preserving safety and effectiveness for these devices and assess whether the costs justify the investment. For devices where updates do not make sense, we need to explore device withdrawal from market and replacement mechanisms.

Healthcare Delivery Organizations

1. It should be a best practice that hospitals maintain Cybersecurity Performance Goals (CPGs) or some type of bar at hospital level to help secure the networks on which these medical devices operate (see Regulator Recommendation #2 – this is a shared recommendation).
2. HDOs must maintain a culture of security throughout their processes, including installing patches issued by device manufacturers and maintaining devices in a manner consistent with the manufacturer's quality systems.
3. HDOs need a comparable regulatory oversight mechanism from an entity like the Joint Commission or CMS. This mechanism can ensure that training, process, and maintenance is performed on practices like the Healthcare Cybersecurity Performance Goals (CPGs). Focus will need to be applied on how hospital networks are secured and how medical devices are segmented on those networks.
4. Many hospitals also have cybersecurity standards for procurement. If these exist, they should be consistently applied.
5. More trained security professionals who can manage legacy devices appropriately, segment networks, understand and manage security risks, and protect the network.
6. Options for funding these efforts include additional reimbursement from CMS for going towards cybersecurity maintenance activities and/or dedicated funding to ensure under-resourced HDOs (the majority of HDO facilities) can be brought up to current best practices.

Suppliers

1. Commit to longer support timeframes so that newly identified vulnerabilities can be patched throughout the lifecycle of the medical device.

Regulators

1. FDA could leverage inspections to ensure medical device manufacturers are following their Postmarket Cybersecurity Guidance recommendations, their associated Quality Systems for addressing postmarket risks with devices currently in use, and their plans for making available updates and patches to medical devices.
2. Congress and/or CMS could provide funding to HDOs to improve their network security, create a better trained workforce, and comply with the Healthcare CPGs to better protect their environment and ensure medical devices are on isolated/segmented networks
3. Update the 2016 FDA Guidance: *Postmarket Management of Cybersecurity in Medical Devices* (Guidance for Industry and Food and Drug Administration Staff) to reflect current best practices on legacy and align with new statutory obligations.

Conclusion

Medical devices and the broader healthcare environment are now more dependent on connectivity than ever before. While this connectivity enables more efficient care, it also introduces a substantial range of cybersecurity risks. If any component of this interconnected system is not properly maintained or managed, the entire environment becomes vulnerable, putting patients, the continuity of care, and healthcare institutions at risk.

Effectively addressing the challenge of legacy medical devices will require sustained attention and resources, particularly in building cybersecurity awareness, training, and technical expertise across all stakeholders. This includes development and maintenance personnel at medical device manufacturers, IT and clinical engineering staff at Healthcare Delivery Organizations (HDOs), and developers and leadership at component and software suppliers whose technologies are integrated into medical devices and healthcare IT systems.

In addition, resolving these issues will require targeted investments across the ecosystem:

- **Medical device manufacturers** should assess existing legacy devices and determine where cybersecurity risks can be reduced and ensure they communicate with customers and follow appropriate risk transfer processes.
- **HDOs** should implement and maintain cybersecurity practices—such as network segmentation, asset management, and alignment with frameworks like the *Healthcare and Public Health Cybersecurity Performance Goals*.
- **Component and software suppliers** should be encouraged to build technologies that are secure by design and can be supported for longer lifecycles, reducing downstream risk to the healthcare sector.

Ultimately, strengthening the cybersecurity of connected medical technologies will require coordinated action across the entire healthcare ecosystem. Addressing the legacy device challenge is not a single-entity task, it is a shared responsibility that will demand strategic investment, collaboration, and accountability at every level.

Mr. BALDERSON. Thank you, Ms. Jump.

Mr. Garcia, 5 minutes.

STATEMENT OF GREG GARCIA

Mr. GARCIA. OK, Mr. Chairman, Ranking Member Clarke, members of the committee, thank you for inviting me to testify about healthcare 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 healthcare, 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 healthcare 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 healthcare 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 healthcare systems that cannot match the firepower 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 (1) 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:]

Health Sector Coordinating Council
Cybersecurity Working Group

Testimony of

Greg Garcia
Executive Director

of the

Healthcare and Public Health Sector Coordinating Council
Cybersecurity Working Group

on

Aging Technology, Emerging Threats:
Examining Cybersecurity Vulnerabilities in Legacy Medical Devices

Before the

United States House of Representatives

Committee on Energy and Commerce

Oversight and Investigations Subcommittee

April 1, 2025

Statement Summary

The Health Sector Coordinating Council Cybersecurity Working Group (CWG) is a government-recognized critical infrastructure industry council of more than 490 healthcare providers, pharmaceutical and medical technology companies, payers, health IT entities and government agencies. We partner to identify and mitigate cyber threats to health data and research, systems, manufacturing and most importantly patient care. The CWG membership collaboratively develops and publishes free healthcare cybersecurity leading practices and policy recommendations, and we produce outreach and communications emphasizing the imperative that ***cyber safety is patient safety***.

We are glad the committee is taking up the important issue of legacy medical device security. This is a complex issue, involving technical, operational and business interdependencies between manufacturers and health providers. And while cyber attacks involving medical devices more often use those devices as portals or jumping off points to other hospital network data and functions, rather than direct attacks on the devices themselves, we cannot ignore the many vulnerabilities in both new and legacy devices.

We cannot ignore how the broader healthcare system is the most targeted now of all critical infrastructure sectors, by both criminal gangs and nation states. This fact requires a more urgent effort on the part of the government to protect health systems that can't match the firepower of nation state cyber trade craft.

For our own part, the CWG has published 5 extensive cybersecurity practices that were negotiated between medical product manufacturers and health providers. These publications guide manufacturers and health systems on how to:

- To 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 that it is a shared responsibility
- To Write model terms and conditions into contracts for the sale and service of medical devices.
- To deliver simple, actionable and consistent cybersecurity vulnerability communications related to products or services.
- To Respond to and recover from cyber incidents that impact computer controlled medical manufacturing, known as operational technology.
- (Soon to come) To Safely and cost effectively patch and update devices while in use in the 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 and interdependent ecosystem. We cannot address the security of our medical device manufacturing in a vacuum. We must also consider how health systems appropriately manage cybersecurity of devices. We must scrutinize the procurement of unregulated software and components that support medical devices and other networked 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 you much good if the steering column is loose and the oil warning light is broken.

I will summarize with recommendations relevant to the importance of medical device security:

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 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 deliberative 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 up to date against cyber threats;

- Development and enforcement of higher standards of "secure by design and 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 can cause systemic risk and cascading damage to patient care and operational resiliency if they are disrupted. Such disrupted workflows can include medical device imaging, diagnostics and therapeutic services; and

- Finally, 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.

Introduction

Chairman Palmer, Ranking Member Clarke, and members of the Committee, my name is Greg Garcia. I am the Executive Director of the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG), an industry-led advisory council of more than 470 healthcare organizations working the U.S. Department of Health and Human Services, CISA and other government agencies to identify and mitigate cybersecurity threats and vulnerabilities to the delivery and support of healthcare. At the heart of this work is a recognition that patient safety must be a guiding principle of healthcare cybersecurity – that *cyber safety is patient safety.*

I appear before you today not with a doctor's bag or a cybersecurity practitioner's toolbox, but as one with 30 years of executive management in the cybersecurity and related professions. I have navigated and advised on the intersecting languages of policy, technology, and business operations and management across the Executive Branch, Congress, and the business community. This includes serving as the nation's first Assistant Secretary for Cybersecurity and Communications at the U.S. Department of Homeland Security from 2006 - 2009, as professional staff on the House Committee on Science where I shepherded the drafting and enactment of the Cybersecurity Research and Development Act of 2002, and as a policy and security executive with high technology and financial services companies and industry groups. In all of these capacities, I am proud of my public service.

We appreciate the Committee's holding this timely hearing to examine health sector cybersecurity of medical technology. My testimony today will focus not on the technical or operational aspects of medical technology security – I will leave that to others on this panel – but on what the health sector and government are doing to strengthen the security and resiliency of the health system and its interconnected ecosystem of subsectors.

Today, I will cover four areas that will help inform both the diagnosis and prescription for healthcare cybersecurity:

First, a brief overview of the Health Sector Coordinating Council Cybersecurity Working Group and our partnership with HHS, CISA and other government agencies;

Second, a review of the cybersecurity challenges and their causes faced by the health sector; and

Third, how we are addressing health sector cybersecurity with a holistic approach.

About the Health Sector Coordinating Council Cybersecurity Working Group

The HSCC Cybersecurity Working Group (CWG) serves as an advisory council to the sector, HHS, CISA, and other government agencies with a critical infrastructure protection mission that has historical recognition promulgated in national policy. Together we identify and mitigate systemic cyber threats to the security and resiliency of critical healthcare infrastructure, develop guidance and policies for mitigating those risks, and facilitate threat preparedness and incident response.

The HSCC CWG is a volunteer organization with a growing list of 460+ member organizations that operate under a charter-based governance structure with an elected Chair, Vice Chair and Executive Committee. Membership is open to organizations that are a) covered entities or business associates under HIPAA; b) health plans or payers; c) regulated by FDA as a medical device or pharmaceutical company; d) health IT companies subject to health data interoperability rules; e) public health organizations and f) any healthcare industry associations or professional societies. A small allotment of "Advisor" members – consulting, law, and security companies - is permitted to participate and support CWG initiatives pro bono.

Where the CWG is focused on best practices policy and long-term strategy, our key operational partner in critical infrastructure protection – the "firefighter" - is the Health Information Sharing and Analysis Center, which is the nation's primary information sharing and incident response organization for the heath sector.

The HSCC CWG is currently organized into numerous function-specific, outcome-oriented task groups composed of 40 to 140 organizations across the health industry and government that develop cybersecurity best-practices and resources for various healthcare cybersecurity disciplines. These disciplines include health provider cybersecurity hygiene; supply chain cyber risk management; workforce development; incident response and operational continuity; and medical technology security, among many others.

With that cross-functional cybersecurity imperative in mind, since 2019 the CWG has published 28 best practices and guidance documents that address the many recommendations of a 2017 HHS healthcare cybersecurity task force of industry and government experts. Those resources, developed by the sector for the sector, are freely available on our website at https://healthsectorcouncil.org/hscc-publications/. Several of these publications are under joint seal by HSCC and HHS as a demonstration of our shared resolve and vision for sound cybersecurity practices that all health organizations should implement. One of these – the

Health Industry Cybersecurity Practices (HICP) - is recognized under P.L. 116-321, signed by President Trump on January 5, 2021, as a set of controls which, if implemented by an entity prior to a breach that becomes subject to HIPAA enforcement action, would be a mitigating factor in the consideration of punitive fines and audits by HHS.

Cyber Threats, Vulnerabilities and Incidents

The reference to "healthcare cybersecurity" was generally not heard ten years ago. But since 2017, when ransomware and other forms of cyberattack disabled the health system in the UK and many other U.S. providers and multinational companies, the epidemic of cyber threats against the health sector has only proliferated, impacting organizations of all sizes across the sector. In 2017, the HHS Healthcare Cybersecurity Task Force report diagnosed healthcare cybersecurity to be in "critical condition."

Threat actors are motivated to leverage ransomware attacks to monetize stolen health data, and operational disruptions. The cybersecurity focus in healthcare has traditionally been on privacy and protection of healthcare data, but when healthcare data is manipulated or destroyed, and health delivery organizations (HDOs), their suppliers, service providers and payment systems are rendered inoperable, as seen in recent ransomware incidents, patient lives can be at risk. This threat is particularly acute for small, rural, critical access and underserved, under-resourced health providers that are operating on razor thin or negative margins and haven't the capability to make the proper investments in cyber preparedness and response programs.

Ransomware and other disruptive cyber attacks

Widely reported incidents experienced over the past few years involved some combination of disruptions affecting patient safety, business operations and clinical workflow, such as:

- Stroke, trauma, cardiac, imaging and other services, closed to admissions, risking patients' lives;
- Radiation and other treatments for cancer patients, including surgery delayed, risking patients' lives;
- Medical records about prescriptions, diagnoses, and therapies become inaccessible and some permanently lost, risking patients' lives;
- Clinical trial data in a research lab, lost;
- Payment systems, down;
- Inability to order or receive supplies;
- Emergency transition to a paper system causing time lags, inefficiencies, and errors potentially risking patients lives;
- Staff furloughed, potentially risking patients' safety; and
- Medical devices stop working, or their settings are corrupted, risking danger to the patient.

Business Risks

In addition to the obvious impact on direct patient care, a cyberattack can inflict health providers and companies with business risks, such as:

- Disruptions to reimbursement and other financial flows
- Damaged reputation
- Lost patient trust
- Lawsuits
- Regulatory penalties
- Strained employee morale and burnout, and
- Reduced stock value.

Medical Device Security in the Healthcare System

Medical devices are a critical component within the overall healthcare ecosystem. Medical devices provide critical capabilities that enable clinicians to better and more efficiently diagnose and treat their patients. These medical devices also represent a potential vulnerability within the healthcare technology environment and may also be impacted when the healthcare technology environment is hit with a cyber attack. Medical devices have become increasingly connected, which provides the ability to provide improved and more efficient health services but also exposes them to additional risks.

From the health provider's perspective:

- Unlike in other sectors, healthcare data must be portable. Sensitive patient information must move between various medical providers, pharmacies, diagnostic facilities, and payers to facilitate proper patient care and payment for those services;
- Many healthcare facilities, such as hospitals, operate in environments that are accessible to the public, which adds to the vulnerability;

- The average patient bed has 15 supporting medical devices, and a 500-bed hospital could have 7,500 devices, many of which are over 8-10 years old and connect to a network that may not be protected or segmented from other systems or databases;
- Thousands of hospital-deployed medical devices are supplied by many different manufacturers with various levels of security and patching protocols. Devices may have unencrypted hard drives or common passwords set by the manufacturer that cannot be changed. Implementing compensating controls, or taking them offline for patches, updates or replacements is complicated. Further complicating health provider replacement programs are budget constraints and small operating margins;
- Correspondingly, a 33% decrease in Medicare Physician payments when adjusted for inflation results in less money for health systems to upgrade or replace aging medical technology;
- Hospitals thus can't afford to purchase new technology routinely due to declining reimbursements and poor margins;
- This causes risk as older, unsecured technology continues to be used;
- This includes devices no longer supported by manufacturers for various reasons, including that they can't get patches from 3rd party software vendors.

And from the device manufacturer's perspective:

- The lifecycle of a medical device is significantly different from other typical IT technology:
    - Medical Device = 7-10 years once purchased

  - Technology (computer, server, phone) = 3 years
- The design and approval process for medtech is also significantly different from other typical IT technology
  - Submissions to FDA for pre-market approval = ~10 years
  - Submissions for updates that "substantially equivalent" in functionality to an existing approved device = ~5-7 years
  - Most unregulated IT devices/tech (including some software used in medtech not under FDA regulatory umbrella) = 1-2 years
- The pricing of medical devices varies widely depending on the device
  - Conventional devices like surgical gloves and routine medical supplies are commodities in competitive markets with high volume and low margin
  - Advanced products (which typically have software and embedded IT tech – like pacemakers and MRIs) are much less competitive, and therefore much more expensive, with higher margins.

Given the above factors, there is regulatory and market fragmentation in the development, approval, acquisition and operational support of medical technology in the clinical environment.

While these observations point to reasoned concern about risks associated with the cybersecurity of medical devices, experience shows that cyber attacks do not typically occur against medical devices specifically but more frequently are the result of 3 prevalent attack methods:

- Social engineering, such as email phishing
- Unpatched vulnerabilities of technology directly facing the internet
- Third party compromise.

That said, any high risk vulnerabilities that are addressable through better product security and implementation practices should indeed be addressed - to reduce risk, protect patient safety, and maintain public confidence in our healthcare system.

We certainly appreciate the committee's interest in the cyber health of the millions of medical devices in the healthcare system that are used to diagnose, monitor and treat patients. The HSCC has spent considerable energy – tens of thousands of collective people hours – developing ways to address cybersecurity challenges inherent in medical device manufacturing and use. Our organizing principle is that technology used in the clinical environment must be secure by design, by default, by demand and by deployment. That makes it a shared responsibility of the manufacturers and the providers. A few points, however, illustrate the complexity of those imperatives:

Through an organizational structure of cross-sector task groups consisting of major healthcare provider systems and medical device manufacturers, the HSCC has since 2019 developed an extensive library of 28 resources and best practices which, if implemented across the sector, would measurably increase the security and resiliency across the sector. Several of these directly address the complexity of medical technology security and accountability. Following is a brief description of these medtech security publications which can be found at https://healthsectorcouncil.org/tag/secure-medtech/:

- **Medical Device and Health IT Joint Security Plan** – a guide for implementing "secure-by-design" and "secure-by-default" principles throughout the product lifecycle of medical devices and health IT solutions. This plan is in its second iteration and has also been used to provide a basis for assessing and improving cybersecurity maturity across the industry.
- **Managing Legacy Technology Security** - a comprehensive guide for medtech manufacturers and health providers to implement cybersecurity in legacy as a shared responsibility in the clinical environment and provides insights for designing future devices that are more secure.
- **Model Contract-Language for Medtech Cybersecurity** - a model contract based on common understandings and reasonable commitments for cybersecurity between health providers and medtech companies at time of sale and during clinical use of the technology.
- **Medtech Vulnerability Communications Toolkit** – provides medical device manufacturers with models for simple, actionable and consistent cybersecurity vulnerability communications related to their products or services.
- **Medical Product Manufacturer Cyber Incident Response Playbook** – a comprehensive guide for medical product manufacturers responding to cyber incidents impacting computer-controlled manufacturing.
- And one more on the way about how best to safely and cost effectively patch and update devices used in the clinical environment.

These publications present negotiated consensus among prominent manufacturers, industry experts, and providers about those cybersecurity management practices to which they agree they should be accountable. And while we continue to improve on implementation and effectiveness of those practices across the health sector, pressures will remain on resource prioritization among both communities, whether it be manufacturer considerations about costs associated with re-engineering, retooling, global third party component sourcing and security, regulatory delay and time to market, or hospital concerns about cybersecurity costs and complexity, attracting and retaining clinical staff, physical facility upkeep and regulatory compliance, and reduced reimbursement pressures.

Given this distressed dynamic, we cannot pursue an imbalanced strategy on just one element or subsector in a broader healthcare ecosystem subject to systemic cyber risk. With multiple healthcare subsectors – providers, payers, medtech, pharma and labs, and health information technology – all subject to varying business models, risk profiles and regulatory requirements, the task before us must be holistic, comprehensive and cross-sector.

Overarching HSCC Cybersecurity Recommendation

Our most immediate recommendation, as submitted to the Administration this week, is that ***the Administration and health sector leaders coordinated by HSCC initiate a structured series of consultations and workshops to forge consensus on a modernized policy for healthcare cybersecurity resiliency, responsibility and accountability.*** Such an approach would operationalize Trump Administration executive orders on *Strengthening the Cybersecurity of*

Federal Networks and Critical Infrastructure in 2017 and *Achieving Efficiency Through State and Local Preparedness* released this month.

Precedent for this innovative approach to cybersecurity policy is in the development of the NIST Cybersecurity Framework as directed in Executive Order 13636 of 2013, "Improving Critical Infrastructure Cybersecurity." This E.O. directed the National Institute of Standards and Technology (NIST) to serve as a convening authority for the private sector to drive development of the Cybersecurity Framework (CSF) for critical infrastructure protection, guided by NIST workshop processes over the prescribed course of one year. The result was *good policy operationalized*: The CSF has grown organically over the past 10 years as the guiding reference for essential cybersecurity practices. It establishes "the What" - expected objectives and measurable outcomes, leaving the industry owners and operators of critical infrastructure to advise and implement "the How" – specific technical, operational and managerial controls tailored for accountability to those promulgated objectives. This approach replaces static one-size-fits-all regulations with guidance that is relevant and scalable to unique sector imperatives, flexible to meet ever-evolving threats and disruptive technology, cost-efficient, and effective at measurably improving cybersecurity outcomes.

Operationalizing the Recommendation

Whether claims processing, lab and blood management or other critical healthcare services we regularly and too often see examples of essential utilities undergirding our critical infrastructure that, if severely disrupted or disabled, would cause cascading and crippling impact on our national economic security and public health and safety. These utilities such as software programs, processing applications and specialty communications platforms are often unknown and taken for granted, but without which the very delivery and financing of healthcare would not be accomplished.

1) Our first operational recommendation, which is now underway and soon to be released, is to ***support and operationalize national health infrastructure mapping and risk assessment*** to provide visibility to those critical services and utilities that support the many interconnected interdependencies across the healthcare ecosystem. There is in fact a policy framework in place – Section 9 of Executive Order 13636 of 2013 - which directs DHS and sector agencies to identify those "critical infrastructure entities where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

   This involves industry leaders from across the healthcare subsectors – health providers and health IT, insurers and plans, pharmaceutical and medical technology companies, and public health agencies -- to identify those critical functions and assets, their connect points and dependencies, the associated concentration risk from mergers and acquisitions, and the relative risk to the provision of healthcare – both immediate impact and duration - that those functions would pose if disrupted. It is about understanding concentration risk, levels of redundancy of similar services, and the adequacy of both physical and cyber protective measures to support the security and resiliency of those critical utilities. This process will take time to get it right, even as it will never be fully accurate given the constantly shifting architecture of our complex healthcare system.

We are in the final stages of phase 1 of this process, which is to create the maps as templates for risk identification and measurement. Phase 2 involves risk measurement methodology and phase 3 is how to manage those risks for a more resilient infrastructure on the premise that *it is not if but when* a disruption will occur. Our expectation is to be done with this effort by this time next year. It needs to be done comprehensively, yet carefully, to ensure that we do not inadvertently reveal critical and potentially vulnerable elements of our critical infrastructure operations to our adversaries.

2) Related to critical function assessment is the imperative to ***hold third party product and service providers and business associates to a higher standard of "secure by design and secure by default"*** for technology services and capabilities used in critical healthcare infrastructure. More than half of all data breaches on health systems are through business associates; many ransomware attacks similarly find their way into enterprise networks through third parties. Many medical devices continue to be delivered to the customer with security vulnerabilities, with uneven attention to the security imperative among device manufacturers.

3) ***Invest in a government-industry rapid response capability.*** Emergency response, recovery and business continuity remain ongoing challenges for private sector and government stakeholders alike. The Change Healthcare attack exposed significant

challenges for health systems to maintain business resiliency and continuity and for government and payers to provide time sensitive operational and financial backup for providers in dire straits. We call it a "Healthcare 911 Cyber Defense": so much of our health system and patient care depend on minutes, hours and days, not on months. Investing in a rapid response force against systemic attacks, using government authority to declare "national cyber emergency", activate catastrophic national cyber insurance to supplement private insurance, provide fast financial support, permit temporary suspension of certain regulatory chokepoints and provide mobile healthcare capability to assist those in dire need, would be a next-generation end-state we call for in our Health Industry Cybersecurity Strategic Plan, discussed below. This need is particularly important for the "target rich, cyber poor" small, rural, critical access, Federally Qualified Health Centers and other underserved, under-resourced health providers across the nation.

4) ***Invest in a cyber safety net for the nation's underserved providers, built on accountability and incentives.*** As discussed, the nation's resourced-constrained health systems are the most vulnerable to cyber threats, lacking the resources and expertise to invest in basic cyber hygiene requirements. Next week, the HSCC will release its report and findings from 40 interviews with resource-constrained provider institutions in 30 states about their cybersecurity challenges and needs from government and the community to meet their cybersecurity obligations to patient safety. While the HSCC has produced so many practical tools to close the

gap between cyber threats and preparedness among the nation's resource-constrained providers, the issue of awareness and resources remain as impediments to adoption and implementation. Many of the smaller, underserved providers in our membership have expressed the same observation that they will invest in strengthened cyber defenses if they are told to do so, but that if given the choice between hiring a nurse to care for patients or hiring a cybersecurity professional, the Hippocratic Oath of "first do no harm" usually wins. But under the principle that "cyber safety is patient safety" many providers would acquiesce to minimum mandatory cyber controls as long as they are financially supplemented.

5) Finally, over the next five years, the industry and government have an all-hands on deck responsibility to ***contribute to achievement of the 5-Year Health Industry Cybersecurity Strategic Plan - https://healthsectorcouncil.org/cyber-strategic-plan/*** published by the HSCC Cybersecurity Working Group in February of last year. The Strategic Plan projects 7 major industry trends in the health sector over the next 5 years and presents a sector-level call to action for healthcare organizations to address those trends and increase their individual and collective cyber resilience for an interconnected industry. The intent of this document is to guide C-suite executives, information technology and security leaders, government and other relevant stakeholders toward investment and implementation of strategic cybersecurity principles which, if adopted, will measurably reduce risks to patient

safety, data privacy, and care operations which can cause significant financial, legal, regulatory, and reputational impact.

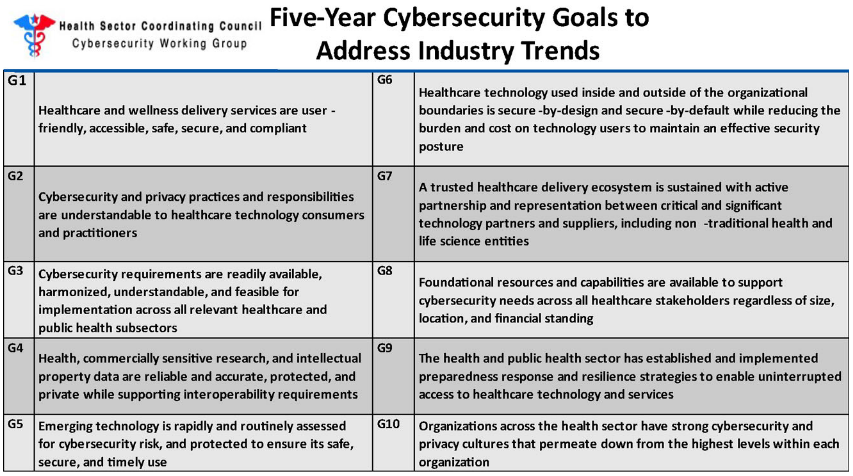
The strategic plan is meant for all HPH sub-sector participants, including medical device manufacturers (MDMs), pharmaceuticals, healthcare delivery organizations (HDOs), health insurance payors, regulators, and other industry and government participants whose products and services are used in healthcare environments.

The plan presents 10 end-state cybersecurity goals, with 12 implementing objectives to achieve those goals by 2029.

If we make progress against the goals and objectives, we can achieve an overall industry target state that looks like:

- Healthcare cybersecurity, both practiced and regulated, is reflexive, evolving, accessible, documented, and implemented for practitioners and patients;
- Secure design and implementation of technology and services across the healthcare ecosystem is a shared and collaborative responsibility;
- Leaders in the healthcare C-Suite embrace accountability for cybersecurity as an enterprise risk and a technology imperative;
- A cyber safety net is in place to ensure that the weaker links in our interconnected ecosystem – those small, rural, critical access and other resource constrained health providers and local public health agencies – are able to ensure a minimum level of good cybersecurity to protect patient safety;

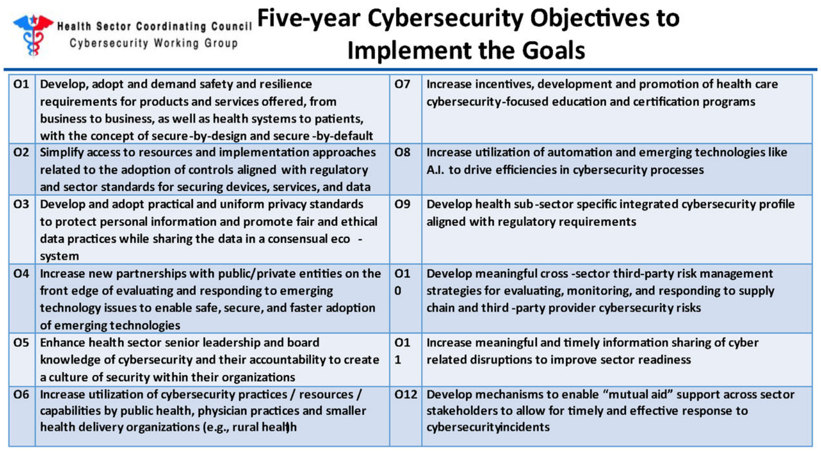
- Workforce cybersecurity learning and practice is a habit for healthcare infrastructure protection; and,
- A “911 Cyber Civil Defense” capability for community early warning, incident response and recovery is reflexive and always on.



Health Sector Coordinating Council
Cybersecurity Working Group

Five-Year Cybersecurity Goals to Address Industry Trends

G1	Healthcare and wellness delivery services are user -friendly, accessible, safe, secure, and compliant	G6	Healthcare technology used inside and outside of the organizational boundaries is secure -by-design and secure -by-default while reducing the burden and cost on technology users to maintain an effective security posture
G2	Cybersecurity and privacy practices and responsibilities are understandable to healthcare technology consumers and practitioners	G7	A trusted healthcare delivery ecosystem is sustained with active partnership and representation between critical and significant technology partners and suppliers, including non -traditional health and life science entities
G3	Cybersecurity requirements are readily available, harmonized, understandable, and feasible for implementation across all relevant healthcare and public health subsectors	G8	Foundational resources and capabilities are available to support cybersecurity needs across all healthcare stakeholders regardless of size, location, and financial standing
G4	Health, commercially sensitive research, and intellectual property data are reliable and accurate, protected, and private while supporting interoperability requirements	G9	The health and public health sector has established and implemented preparedness response and resilience strategies to enable uninterrupted access to healthcare technology and services
G5	Emerging technology is rapidly and routinely assessed for cybersecurity risk, and protected to ensure its safe, secure, and timely use	G10	Organizations across the health sector have strong cybersecurity and privacy cultures that permeate down from the highest levels within each organization



Health Sector Coordinating Council
Cybersecurity Working Group

Five-year Cybersecurity Objectives to Implement the Goals

O1	Develop, adopt and demand safety and resilience requirements for products and services offered, from business to business, as well as health systems to patients, with the concept of secure-by-design and secure -by-default	O7	Increase incentives, development and promotion of health care cybersecurity-focused education and certification programs
O2	Simplify access to resources and implementation approaches related to the adoption of controls aligned with regulatory and sector standards for securing devices, services, and data	O8	Increase utilization of automation and emerging technologies like A.I. to drive efficiencies in cybersecurity processes
O3	Develop and adopt practical and uniform privacy standards to protect personal information and promote fair and ethical data practices while sharing the data in a consensual eco - system	O9	Develop health sub -sector specific integrated cybersecurity profile aligned with regulatory requirements
O4	Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies	O10	Develop meaningful cross -sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third -party provider cybersecurity risks
O5	Enhance health sector senior leadership and board knowledge of cybersecurity and their accountability to create a culture of security within their organizations	O11	Increase meaningful and timely information sharing of cyber related disruptions to improve sector readiness
O6	Increase utilization of cybersecurity practices / resources / capabilities by public health, physician practices and smaller health delivery organizations (e.g., rural heal)h	O12	Develop mechanisms to enable "mutual aid" support across sector stakeholders to allow for timely and effective response to cybersecurityincidents

The Cybersecurity Strategic Plan is the result of extensive and multiple collaborative sessions among almost 200 industry and government organizations across the HPH sector represented by senior cybersecurity and clinical executives and subject matter experts over a period of over 18 months.

Conclusion

Mr. Chairman, Members of the Committee, as a critical infrastructure industry the health sector and its dedicated workforce are mobilizing against the ongoing and existential threat of cyber disruption. We also recognize we need to move faster to keep up with the evolving threats. But through continued and expanded engagement in our collective purpose, broader awareness promotion, and forward-leaning government programs and support, we can move the needle and five years from now upgrade the healthcare cybersecurity diagnosis from "critical" to "stable condition."

Thank you.

Submitted for the record:

- Health Industry Cybersecurity Strategic Plan - https://healthsectorcouncil.org/the-plan/
- HSCC cybersecurity policy, programmatic and regulatory recommendations for government consideration - https://healthsectorcouncil.org/health-industry-cybersecurity-recommendations-for-government-policy-and-programs/

Mr. BALDERSON. Thank you, Mr. Garcia.

Dr. Fu, 5 minutes, please.

STATEMENT OF KEVIN FU, PH.D.

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 healthcare 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 Healthcare 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 hijack infusion pumps to administer incorrect dosages. Without proactive cybersecurity measures, including postmarket 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 premarket, but needs to also focus on postmarket risk management.

Moreover, in my testimony to this committee 9 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. Postmarket 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 premarket review team. But these are often nonreview 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:]

Statement of Prof. Kevin Fu, Ph.D.

Northeastern University; Boston, MA

College of Engineering
Departments of Electrical and Computer Engineering & Bioengineering; the Khoury College of Computer Sciences; the Kostas Research Institute (KRI) for Homeland Security; and Archimedes Center for Healthcare and Medical Device Cybersecurity

Hospital Cybersecurity and Legacy Medical Devices: Fine Wine or Spoiled Milk?

Submitted to the U.S. House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations Hearing on
“Aging Technology, Emerging Threats:
Examining Cybersecurity Vulnerabilities in Legacy Medical Devices”
Tuesday, April 1, 2025

Executive Summary

Legacy medical devices are inherently insecure, relying on outdated and unsupported software that leave them vulnerable to cyber threats. Essential for patient care, if compromised these devices can disrupt hospitals, adulterate cancer radiation therapy, or cause drug infusion pumps to administer incorrect dosages. Although regulatory efforts have improved medical device cybersecurity, many legacy systems remain unprotected. Flaws in the Contec patient monitor highlight how poor engineering can create significant post-market risks in already cleared devices. The FDA should have greater post-market capabilities to regulate legacy medical devices for cybersecurity risks, as ongoing scrutiny is necessary to protect patient health and prevent nationwide outages of healthcare delivery.

I recommend three actions to improve legacy medical device cybersecurity. First, FDA should grow its cybersecurity expertise to better manage post-market vulnerabilities and emerging threats. Second, Software Bills of Materials (SBOMs) should be strongly encouraged for legacy medical devices to improve cybersecurity incident preparedness. Third, I urge the establishment of national-scale testing facilities, modeled after the NTSB or automotive crash testing, to evaluate medical device security through whole-hospital simulation. These steps enhance national security, promote innovation, and protect patient care.

1. Introduction.

Good morning, Chairmen Guthrie and Palmer, Ranking Members Pallone and 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 over 30 years working in healthcare and cybersecurity, and 18 years of fundamental research on medical device cybersecurity. This includes my previous experience as the inaugural Acting Director of Medical Device Security at FDA's Center for Devices and Radiological Health (CDRH).

2. Credentials and Experience.

My name is Dr. Kevin Fu. I represent the academic and healthcare cybersecurity research communities. I am a professor at Northeastern University[1] where I teach medical device security engineering[2] and serve as the Director of the Archimedes Center for Healthcare and Medical Device Cybersecurity. I conduct research on embedded security—the discipline of protecting computers built into every day objects ranging from pacemakers to cars to drug manufacturing. In

[1] Northeastern University is a global campus system in the United States, Canada, and London with a focus on an experiential learning model, high-impact research, deep partnerships, and worldwide reach.

[2] https://spqrlab1.github.io/medcybersecurity/

1993, I worked at a community hospital in Holland, Michigan which introduced me to the challenges and opportunities of maintaining legacy systems in hospitals.

My educational qualifications include a Ph.D., master's degree, and bachelor's degree from the MIT Department of Electrical Engineering and Computer Science. I am speaking today as an individual. All opinions, findings, and conclusions are my own and do not necessarily reflect the views of any of my past or present sponsors or employers.

3. 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 without physical contact[3]. 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 hijack infusion pumps to administer incorrect doses.

[3] "A Heart Device Is Found Vulnerable to Hacker Attacks" by Barnaby J. Feder. In The New York Times, Mar 12, 2008. https://www.nytimes.com/2008/03/12/business/12heart-web.html
"Of Fact, Fiction and Cheney's Defibrillator" by Gina Kolata. In The New York Times, Oct 27, 2013. https://www.nytimes.com/2013/10/29/science/of-fact-fiction-and-defibrillators.html

Without proactive cybersecurity measures, including post-market oversight, we risk turning life-saving equipment into attack surfaces that endanger patient safety.

A. Legacy Medical Devices Are Inherently Insecure

A legacy medical device is one that is not merely insecure, but is insecurable. Its software cannot be patched. It is the difference between an unbuckled seatbelt versus a car without any seatbelts at all—unsafe at any speed. While these devices are vital to patient care, many lack the necessary security features to defend against modern threats. They often operate on outdated 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 cybersecurity can have life-or-death consequences.

B. Progress in Medical Device Security

While regulatory and legislative progress has been made to improve medical device security, vulnerabilities still arise, often targeting the weakest link: outdated legacy technology. The pace of advancement has not fully kept up with the evolving sophistication of cyber threats.

C. Cybersecurity Issues in the Contec Patient Monitor

The cybersecurity flaws in the Contec patient monitor are likely a result of poor engineering rather than malice. Applying Hanlon's Razor—never attribute to malice what is adequately explained by stupidity. Short of a wider pattern of subterfuge by a manufacturer, it seems that these flaws are due to negligence. Indeed, history has shown that shoddy engineering in rebranded Chinese products appear driven by business economics rather than subterfuge[4]. However, this does not excuse the lack of proper cybersecurity controls, which pose significant risks to patient safety, regardless of the intent. Hardcoded default passwords and network addresses in some medical devices are a prime example of egregious security lapses. These devices are born insecure by default, creating unnecessary risks.

D. The Importance of FDA Scrutiny for Legacy Medical Devices

A key lesson from the Contec advisory is that FDA scrutiny of legacy medical devices should not exclude devices that were previously cleared. Some medical device manufacturers have argued that certain cybersecurity requirements should not retroactively apply to older devices. However, the Contec advisory illustrates why exempting legacy devices from cybersecurity requirements is

[4] https://www.bunniestudios.com/blog/on-microsd-problems/

detrimental to patient safety. Grandfathered medical devices should not be exempt from security considerations if the goal is to ensure timely, safe, and effective healthcare whether in cardiac monitoring, cancer radiation therapy, or other critical treatments and diagnoses.

E. Need for Independent Testing Facilities for Whole-Hospital Simulation

In my testimony to this Committee nine years ago[5], I emphasized that the nation lacks independent, large-scale testing facilities, such as those comparable to the NTSB (for post-market testing), automotive crash safety testing (for pre-market evaluation), or NNSS (for destruction and survivability testing). Such proving grounds are essential for evaluating the cybersecurity defenses of medical devices in whole-hospital environments.

F. Lack of Visibility and Security Posture Awareness

In a 2018 letter to this Committee[6], I highlighted how hospitals struggle to identify which devices are in use, let alone assess their security postures. Without visibility into the software and components that make up a device—a challenge that Software Bills of Materials (SBOM) seek to address—healthcare providers are left operating in the dark when new vulnerabilities emerge.

[5] https://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-FuK-20161116.pdf

[6] https://spqrlab1.github.io/papers/Fu-Archimedes-House-EC-supported-lifetimes-2018.pdf

G. Cybersecurity as a Solution, Not a Problem

Cybersecurity is not the problem; it is the solution. Robust security measures will enable new markets, promote innovation, and foster consumer confidence in the use of technologies that improve quality of life. Conversely, poor security can erode trust, leading patients and clinicians to lose confidence in technological solutions.

4. Recommendations

I offer three key recommendations to manage cybersecurity risks from legacy medical devices:

A. 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. These cybersecurity staff crucial to national security are not necessarily pre-market reviewers, but are often **non-review staff** who monitor for and manage newly discovered post-market vulnerabilities and incidents. These subject matter experts (SMEs) are essential for evaluating 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.

i. Support agencies such as HHS/FDA, DHS/CISA, DOC/NIST, and NSF to advance our understanding of how to protect legacy medical devices and to establish a cybersecurity workforce that meets medical device industry needs.

ii. Help the FDA retain and recruit cybersecurity talent, not just for pre-market reviewers, but also for post-market management of legacy medical security vulnerabilities and incidents that otherwise will lead to patient injury and harm.

B. Require or Strongly Incentivize Software Bills of Materials (SBOMs)

SBOMs should be required for all new devices and strongly encouraged for legacy devices. These inventories allow stakeholders—including manufacturers, regulators, and hospitals—to rapidly assess whether they are affected by newly discovered software vulnerabilities or exploits.

C. Support Shared Testing Infrastructure for Embedded Cybersecurity

Study the feasibility of standing up an independent, national embedded cybersecurity testing facility modeled after the NTSB, automotive crash safety testing, or the Nevada National Security Site. The U.S. needs a national-scale, independent facility akin to the NTSB or crash test labs—where healthcare providers, manufacturers, and researchers can collaboratively evaluate the security of complex, interoperable medical systems. The cost of not doing so is borne daily by the 6,000+ hospitals each repeating duplicative risk assessments on individual medical devices without shared resources and without the rigor of a whole-hospital simulation.

5. Summary

Legacy medical devices run on outdated software, making them vulnerable to attacks that can threaten patient safety. It is important to preserve and increase FDA's in-house cybersecurity subject matter expertise, not just for medical device reviewing, but also post-market management of vulnerabilities and incidents. Finally, I recommend establishing a National Technical Means in the form of testing facilities to evaluate medical device security through whole-hospital simulation.

Cybersecurity is not a barrier to innovation. It is a foundation. It enables trust in medical technologies, ensures continuity of patient care, and protects public confidence in our healthcare infrastructure. We cannot treat cybersecurity as an afterthought. It must be embedded throughout the entire lifecycle of a medical device from design to decommissioning. Legacy medical device security is spoiled milk, not fine wine. It does not age gracefully.

I thank the Committee for your leadership and attention to this important matter and am happy to support your efforts going forward.

Respectfully submitted,

Kevin Fu

Kevin Fu, Ph.D.
Director, Archimedes Center for Healthcare and Medical Device Cybersecurity
Professor,
Departments of Electrical & Computer Engineering and Bioengineering
College of Engineering
Khoury College of Computer Sciences
Kostas Research Institute (KRI) for Homeland Security
archimedes@northeastern.edu
secure-medicine.org
spqrlab1.github.io

Biography

Dr. Kevin Fu, Ph.D., is Professor of Electrical & Computer Engineering, the Khoury College of Computer Sciences, and Bioengineering at Northeastern University in Boston where he directs the Archimedes Center for Healthcare and Medical Device Cybersecurity. He is also a faculty member at the Kostas Research Institute (KRI) for Homeland Security. His laboratory protects medical devices from cybersecurity threats that could otherwise disrupt patient care. Fu's 2008 research on vulnerabilities in implantable cardiac defibrillators prompted improvements at medical device manufacturers, global regulators, and international safety standards bodies. His pacemaker research also inspired an episode of Homeland. Before joining Northeastern University, Fu served as the inaugural Acting Director of Medical Device Security at FDA's Center for Devices and Radiological Health (CDRH) and program director for cybersecurity at FDA's Digital Health Center of Excellence. Fu received his B.S., M.Eng., and Ph.D. from MIT.

Fu's work has earned him honors, including ACM Fellow, IEEE Fellow, AAAS Fellow, Sloan Research Fellow, MIT Technology Review TR35 Innovator of the Year, a Fed100 Award, and an NSF CAREER Award. He also received an IEEE Security & Privacy Test of Time Award for his pacemaker security research, as well as best paper awards from USENIX Security, IEEE Security & Privacy, and ACM SIGCOMM. Fu has testified in the House and Senate on matters of information security and was commissioned by the National Academy of Medicine to publish a report on trustworthy medical device software. He served as the co-chair of the AAMI cybersecurity working group to create the first FDA-recognized consensus standards to improve the security of medical device manufacturing. Fu advises medical device and pharmaceutical manufacturers on cybersecurity regulations for operational technology.

Mr. PALMER [presiding]. I thank the witnesses for your testimony, and we will now move to questioning. I will begin and recognize myself for 5 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. healthcare 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 nonlegacy 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. Yes. 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. Yes. Mr. Garcia, how does the widespread use of legacy medical devices make healthcare 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's 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 healthcare 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 postmarket 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 postmarket surveillance?

Dr. FU. Yes, I believe it does. It would be difficult with any kind of staffing reduction to manage the postmarket or premarket 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 postmarket 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 5 minutes for his questions.

Mr. GUTHRIE. 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 prepositioning 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.

Mr. GUTHRIE. 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——

Mr. GUTHRIE. 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——

Mr. GUTHRIE. 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 healthcare, that can cause a problem and it can cause disruption in a society.

Mr. GUTHRIE. But it is also for espionage as well, right?

Ms. JUMP. Sure, yes.

Mr. GUTHRIE. 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.

Mr. GUTHRIE. 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.

Mr. GUTHRIE. 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 2 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.

Mr. GUTHRIE. OK, 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's 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.

Mr. GUTHRIE. OK. 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 5 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 healthcare across the Nation, and if we are going to be able to respond effectively to a 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. OK, 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 5 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 multifactorial.

So number one, they don't have the latest and greatest medical technology 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 an 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 3 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 has 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 [continuing]. 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 5 minutes for her questions.

Mrs. TRAHAN. Thank you to the Chair, thank you to the ranking member and for our witnesses here today.

Just a 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, derisking 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 5 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. OK.

Ms. JUMP [continuing]. 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 prepositioning 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 healthcare. 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 healthcare. We are the most commonly targeted critical healthcare—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 followup 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 5 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 postmarket 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 healthcare 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 2 hours a year, but it was down for 6 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 healthcare 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 healthcare 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 postmarket 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 5 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. OK, 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 manufacturer 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 2, 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. OK, 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 5 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. Yes, 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 preproduct that was described earlier, prebusiness. 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 5 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 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 a device is identified, what tools are available to inform the public and providers who may be using the 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 5 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 premarket and postmarket, and maybe give you an example of an incident management.

So premarket, 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 postmarket 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 6 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 healthcare 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 5 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 2 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. Yes. So this is a people and process problem. And there—what I will say is this: Inside healthcare we have been underresourced 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. OK.

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. OK, all right. You got the Cyber Center of Excellence——

Mr. DECKER. Yes.

Mr. ALLEN [continuing]. 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. OK.

Mr. DECKER [continuing]. Health and Human Services and CISA. Those have been the two main entry points into the dialog.

Mr. ALLEN. OK. So might this be a means and methods problem?

Mr. DECKER. Yes. Yes, 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. Yes.

Mr. ALLEN [continuing]. 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 healthcare, 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, OK? 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 5 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. OK. 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. healthcare 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. OK, that's all. I just wanted a clarification.

The Chair now recognizes the gentleman from Ohio, Mr. Rulli, for 5 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 healthcare 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 cochair of an initiative that created the Health Industry Cybersecurity Practices, or HICP. Volume 1 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 healthcare 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 5 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 2½ 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 2 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 5 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 healthcare ecosystem—

Mr. FULCHER. Healthcare. So——

Mr. GARCIA [continuing]. Not just medical devices.

Mr. FULCHER. OK, so why healthcare?

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

Mr. GARCIA. Yes, 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 healthcare is, first off, it is a widely distributed, multifaceted 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. OK. 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 healthcare 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 healthcare.

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. Yes.

Mr. FULCHER [continuing]. 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. Yes. We actually have an answer, an answer that we've been working on for the last 8 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. OK. 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 healthcare 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 5 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 and 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 postmarket 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 healthcare 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 5 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 healthcare, 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 healthcare, up to and including cybersecurity.

Mr. JOYCE. Should there be?

Dr. DAMEFF. That is an 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 is 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 appears at the conclusion of the hearing.]

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.]

[Material submitted for inclusion in the record follows:]

U.S. Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
“Aging Technology, Emerging Threats: Examining Cybersecurity Vulnerabilities in Legacy Medical Devices”
April 1, 2025
Documents for the Record

1. A letter addressed to the Honorable Robert F. Kennedy Jr., from Ranking Member Pallone, Ranking Member DeGette, and Ranking Member Clarke, submitted by the Minority.
2. A letter addressed to Sara Brenner, Acting Commissioner of Food and Drugs at the U.S. Food and Drug Administration, from Peter Marks, Director at the Center for Biologics Evaluation and Research at the U.S. Food and Drug Administration, submitted by the Minority.
3. A statement from AdvaMed entitled “AdvaMed Statement on Reports of Significant FDA Jobs Cuts,” submitted by the Minority.

BRETT GUTHRIE, KENTUCKY
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED NINETEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-3641
Minority (202) 225-2927

April 1, 2025

The Honorable Robert F. Kennedy, Jr.
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue SW
Washington, D.C. 20201

Dear Secretary Kennedy:

We write to express our outrage at your reckless announcement terminating nearly 25 percent of the workforce at the Department of Health and Human Services (HHS) and to seek information about this decision, which you have not provided to Congress. Last week, you announced that HHS would be eliminating 10,000 jobs on top of the 10,000 public servants who have already been terminated, or who have taken the deferred resignation program. This is an alarming, irresponsible, DOGE-driven attempt to dismantle an entire department and its critical work in order to fund giant tax breaks for the wealthy. It is also a blatant effort to push out doctors and scientists whose work has been grounded in real science but that runs counter to your dangerous agenda of misinformation.

These layoffs and hastily concocted plans to restructure HHS will harm all Americans who rely on the expertise and efforts of staff across HHS for safe and effective medical products, for the delivery of essential healthcare services, and for the protection of public health and the advancement of biomedical research. To claim to want to make "America Healthy Again" and then dismiss 25percent of the people who work at HHS without regard to the impact these cuts will have on the American people is pure hypocrisy. Already, experts and organizations dedicated to public health have raised the alarm, calling the planned cuts "dangerous," "deeply misguided," and "preposterous."[1]

This announcement comes on the heels of a round of terminations of probationary employees in February that was not only illegal but also led to a substantial number of

[1] Doctors for America, *Doctors for America Condemns HHS Cuts* (March 28, 2025) (press release); Stat+, *Former HHS Secretary Donna Shalala on the Agency's 'Silly New Bureaucracy'* (Mar. 27, 2025) (https://www.statnews.com/2025/03/27/hhs-cuts-rfk-jr-kennedy-reorgnization-layoffs-donna-shalala-criticism/); *RFK Jr. Plans 10,000 Job Cuts in Major Restructuring of Health Department*, The Wall Street Journal (Mar. 27, 2025).

employees being asked to return once you and others at HHS realized they were indeed essential to HHS's mission.[2] Some HHS operating divisions are already struggling to maintain efficiency and quality after the February DOGE-led cuts. At the Food and Drug Administration (FDA), for example, scientists now have double the number of product applications to review as a result of those terminations, and the pace of review of new drug applications has slowed significantly.[3] The Department is also losing swaths of highly experienced leaders who resigned or refused to return to HHS even if their terminations were rescinded.[4] Appallingly, more experts are being forced to resign because they do not align with your misguided agenda, including your deeply misguided determination to set public health back a century by questioning the settled science regarding the safety and efficacy of vaccines.[5] We are concerned that your efforts will result in the resurgence of long eradicated diseases and the unnecessary deaths of many Americans to vaccine preventable diseases.

This is no time to carelessly eviscerate our health workforce. There is an ongoing risk of avian flu outbreaks and more cases of measles already this year than in the past five years.[6] Americans deserve the benefit of numerous treatments and cures that are being diligently researched and examined through clinical trials at NIH and elsewhere within HHS. They also deserve access to safe and effective medical products that are reviewed by FDA within the congressionally mandated timelines. Further, seniors and people with disabilities deserve the opportunity to live independently and participate in their communities—yet, you have carelessly cut the Administration for Community Living (ACL), which is the only federal agency specifically focused on this need.

Since you chose to provide only a six-minute video devoid of meaningful detail on this major announcement, Congress is left entirely without crucial information.[7] It is unacceptable that you refused to provide a briefing to the Committee or answer any questions regarding this proposed reorganization and layoffs – after all, Congress must approve many of the decisions

[2] Fierce Healthcare, *Federal Union Draws Up Lawsuit Over Trump EO as RFK Jr. Readies 10,000 HHS Cuts* (https://www.fiercehealthcare.com/regulatory/rfk-jr-prepares-10000-job-cuts-across-hhs-new-wave-worker-reductions) (Mar. 28, 2025).

[3] Reuters, *Exclusive: FDA Staff Struggle to Meet Product Review Deadlines After DOGE Layoffs* (Mar. 27, 2025) (https://www.reuters.com/business/healthcare-pharmaceuticals/fda-staff-struggle-meet-product-review-deadlines-after-doge-layoffs-2025-03-27/).

[4] CBS News, *Top FDA Food Safety Official's Resignation Letter Warns Firings Will Backfire on RFK Jr.* (Feb. 20, 2025) (https://www.cbsnews.com/news/fda-food-safety-james-jones-resigns-warning-rfk-jr/).

[5] *Top F.D.A. Vaccine Official Resigns, Citing Kennedy's 'Misinformation and Lies',* The New York Times (Mar. 28, 2025).

[6] Centers for Disease Control and Prevention, *Measles Cases and Outbreaks* (Mar. 28, 2025) (https://www.cdc.gov/measles/data-research/index.html#cdc_data_surveillance_section_5-yearly-measles-cases); Centers for Disease Control and Prevention, *H5 Bird Flu: Current Situation* (Mar. 28, 2025) (https://www.cdc.gov/bird-flu/situation-summary/index.html).

[7] Secretary Kennedy (@SecKennedy), X (Mar. 27, 2025, 9:00 AM) (x.com/SecKennedy/status/1905243470366670926).

that you proposed. It is simply unclear what authority allows you to make these sweeping changes without congressional approval, and you have not provided that information.

As former Director of FDA's Center for Biologics Evaluation and Research Peter Marks wrote in his resignation letter last week, "[I]t has become clear that truth and transparency are not desired by the Secretary, but rather he wishes subservient confirmation of his misinformation and lies."[8] We demand truth and transparency, and we therefore require that you provide written answers to the following requests by April 15 and provide a briefing for Committee staff shortly thereafter.

1. Please provide a detailed list of the roles being eliminated across HHS. For each, provide:

    a. The title of the role;

    b. The operating division and office in which that role currently exists;

    c. A description of that role;

    d. How the work being performed by that role will be reassigned;

    e. Whether that role is currently occupied, and if so, whether the individual in that role will be terminated from or reassigned in HHS;

    f. What date that termination or reassignment will occur; and

    g. The statutory authority that provides the basis for these mass terminations, as well as the statutory authority that provides the basis for eliminating entire operating divisions of HHS, such as the Substance Abuse and Mental Health Services Administration (SAMHSA) and Health resources and Services Administration (HRSA), which have detailed and specific statutory responsibilities laid out in the Public Health Service Act.

2. Please describe in detail the process by which you determined what roles would be eliminated and produce all supporting documentation. Include in your answer:

    a. The individuals involved in deciding which roles would be eliminated, including their title and the agency for which they work;

    b. The criteria used to determine what roles could be eliminated;

[8] *Top Vaccine Official Resigns from FDA, Criticizes RFK Jr. for Promoting 'Misinformation and Lies'*, Associated Press (Mar. 29, 2025).

c. The process for deciding whether the work conducted by a role would be reassigned or eliminated entirely;

d. Any risk assessments involved in determining whether a role was necessary for public health and safety and the individuals involved in conducting and reviewing those assessments;

e. What feedback, if any, was sought by leaders within operating divisions and offices as part of the process;

f. What feedback, if any, was provided by individuals outside of HHS;

g. What feedback, review, or consultation was provided by non-governmental organizations, contractors, consultants, or other non-federal entities or employees; and

h. Any impact analyses conducted by HHS of the impact these terminations will have on the ability of each operating division to meet its statutory responsibilities to the American people.

3. A fact sheet circulated by HHS states that the elimination of roles at FDA "will not affect drug, medical device, or food reviewers, nor will it impact inspectors."[9] Please specify what is meant by the elimination of 3,500 roles at FDA not "affect[ing] reviewers" or "impact[ing] reviewers."

4. The fact sheet circulated by HHS states that the reduction of 1,200 individuals at NIH will result from "centralizing procurement, human resources, and communications across its 27 institutes and centers."[10] Please confirm that this means that no other staff aside from those in purely procurement, human resources, or communications roles will be eliminated from NIH. To the extent that this is not accurate, please detail what other roles will be eliminated and why those were not described in the fact sheet.

5. The fact sheet circulated by HHS states that "programs within the Administration for Community Living (ACL) that support older adults and people of all ages with disabilities will be split across the Administration for Children and Families (ACF), Assistant Secretary for Planning and Evaluation (ASPE), and Centers for Medicare and Medicaid Services (CMS)." Please clarify specifically which programs will be transferred to which agencies and whether HHS is eliminating ACL employees, programs, and/or functions as part of this action.

[9] U.S. Department of Health and Human Services, *Fact Sheet: HHS' Transformation to Make America Healthy Again* (Mar. 27, 2025) (press release).

[10] *Id.*

6. Please specify which five regional offices will be closed and the process for determining why regional offices should be closed and which ones should be closed.

7. Please specify which operating divisions will be eliminated or consolidated. For each, please specify which new or existing operating division(s) will be responsible for carrying out the eliminated or consolidated operation division's work.

If you have any questions about this request, please contact the Committee Democratic staff at (202) 225-2927.

Sincerely,

Frank Pallone, Jr.

Frank Pallone, Jr.
Ranking Member

Diana DeGette

Diana DeGette
Ranking Member
Subcommittee on Health

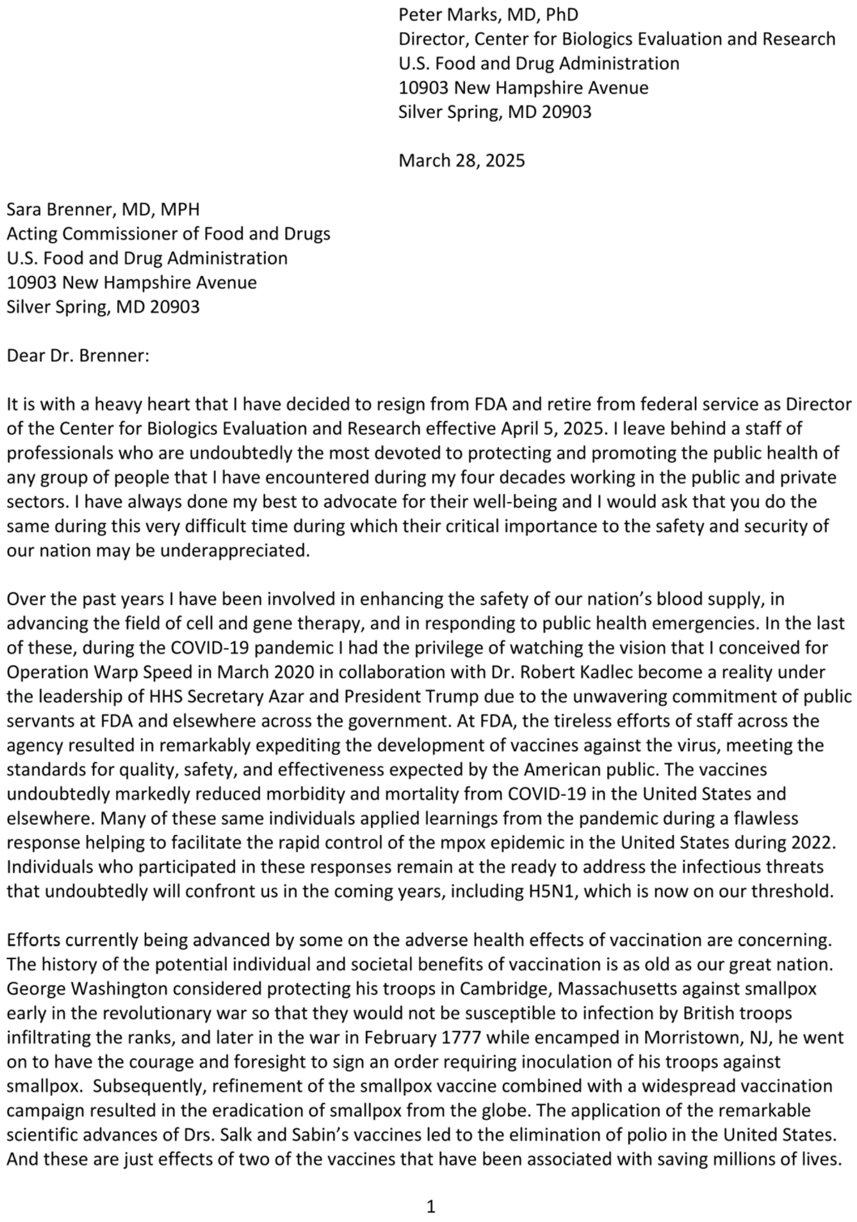
Yvette D. Clarke M.C.

Yvette D. Clarke
Ranking Member
Subcommittee on Oversight
and Investigations

cc: The Honorable Brett Guthrie
Chairman

The Honorable Buddy Carter
Chairman
Subcommittee on Health

The Honorable Gary Palmer
Chairman
Subcommittee on Oversight and Investigations



Peter Marks, MD, PhD
Director, Center for Biologics Evaluation and Research
U.S. Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20903

March 28, 2025

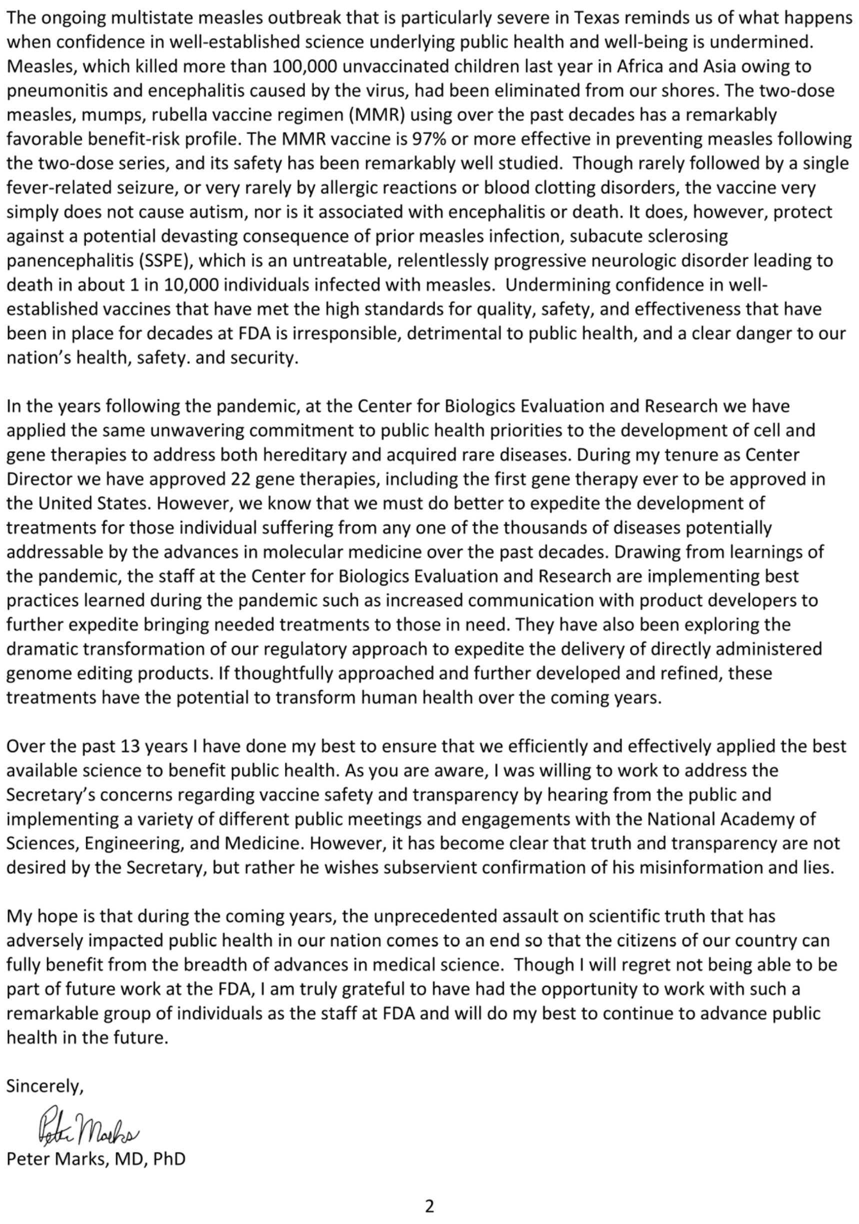
Sara Brenner, MD, MPH
Acting Commissioner of Food and Drugs
U.S. Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20903

Dear Dr. Brenner:

It is with a heavy heart that I have decided to resign from FDA and retire from federal service as Director of the Center for Biologics Evaluation and Research effective April 5, 2025. I leave behind a staff of professionals who are undoubtedly the most devoted to protecting and promoting the public health of any group of people that I have encountered during my four decades working in the public and private sectors. I have always done my best to advocate for their well-being and I would ask that you do the same during this very difficult time during which their critical importance to the safety and security of our nation may be underappreciated.

Over the past years I have been involved in enhancing the safety of our nation's blood supply, in advancing the field of cell and gene therapy, and in responding to public health emergencies. In the last of these, during the COVID-19 pandemic I had the privilege of watching the vision that I conceived for Operation Warp Speed in March 2020 in collaboration with Dr. Robert Kadlec become a reality under the leadership of HHS Secretary Azar and President Trump due to the unwavering commitment of public servants at FDA and elsewhere across the government. At FDA, the tireless efforts of staff across the agency resulted in remarkably expediting the development of vaccines against the virus, meeting the standards for quality, safety, and effectiveness expected by the American public. The vaccines undoubtedly markedly reduced morbidity and mortality from COVID-19 in the United States and elsewhere. Many of these same individuals applied learnings from the pandemic during a flawless response helping to facilitate the rapid control of the mpox epidemic in the United States during 2022. Individuals who participated in these responses remain at the ready to address the infectious threats that undoubtedly will confront us in the coming years, including H5N1, which is now on our threshold.

Efforts currently being advanced by some on the adverse health effects of vaccination are concerning. The history of the potential individual and societal benefits of vaccination is as old as our great nation. George Washington considered protecting his troops in Cambridge, Massachusetts against smallpox early in the revolutionary war so that they would not be susceptible to infection by British troops infiltrating the ranks, and later in the war in February 1777 while encamped in Morristown, NJ, he went on to have the courage and foresight to sign an order requiring inoculation of his troops against smallpox. Subsequently, refinement of the smallpox vaccine combined with a widespread vaccination campaign resulted in the eradication of smallpox from the globe. The application of the remarkable scientific advances of Drs. Salk and Sabin's vaccines led to the elimination of polio in the United States. And these are just effects of two of the vaccines that have been associated with saving millions of lives.



The ongoing multistate measles outbreak that is particularly severe in Texas reminds us of what happens when confidence in well-established science underlying public health and well-being is undermined. Measles, which killed more than 100,000 unvaccinated children last year in Africa and Asia owing to pneumonitis and encephalitis caused by the virus, had been eliminated from our shores. The two-dose measles, mumps, rubella vaccine regimen (MMR) using over the past decades has a remarkably favorable benefit-risk profile. The MMR vaccine is 97% or more effective in preventing measles following the two-dose series, and its safety has been remarkably well studied. Though rarely followed by a single fever-related seizure, or very rarely by allergic reactions or blood clotting disorders, the vaccine very simply does not cause autism, nor is it associated with encephalitis or death. It does, however, protect against a potential devasting consequence of prior measles infection, subacute sclerosing panencephalitis (SSPE), which is an untreatable, relentlessly progressive neurologic disorder leading to death in about 1 in 10,000 individuals infected with measles. Undermining confidence in well-established vaccines that have met the high standards for quality, safety, and effectiveness that have been in place for decades at FDA is irresponsible, detrimental to public health, and a clear danger to our nation's health, safety. and security.

In the years following the pandemic, at the Center for Biologics Evaluation and Research we have applied the same unwavering commitment to public health priorities to the development of cell and gene therapies to address both hereditary and acquired rare diseases. During my tenure as Center Director we have approved 22 gene therapies, including the first gene therapy ever to be approved in the United States. However, we know that we must do better to expedite the development of treatments for those individual suffering from any one of the thousands of diseases potentially addressable by the advances in molecular medicine over the past decades. Drawing from learnings of the pandemic, the staff at the Center for Biologics Evaluation and Research are implementing best practices learned during the pandemic such as increased communication with product developers to further expedite bringing needed treatments to those in need. They have also been exploring the dramatic transformation of our regulatory approach to expedite the delivery of directly administered genome editing products. If thoughtfully approached and further developed and refined, these treatments have the potential to transform human health over the coming years.

Over the past 13 years I have done my best to ensure that we efficiently and effectively applied the best available science to benefit public health. As you are aware, I was willing to work to address the Secretary's concerns regarding vaccine safety and transparency by hearing from the public and implementing a variety of different public meetings and engagements with the National Academy of Sciences, Engineering, and Medicine. However, it has become clear that truth and transparency are not desired by the Secretary, but rather he wishes subservient confirmation of his misinformation and lies.

My hope is that during the coming years, the unprecedented assault on scientific truth that has adversely impacted public health in our nation comes to an end so that the citizens of our country can fully benefit from the breadth of advances in medical science. Though I will regret not being able to be part of future work at the FDA, I am truly grateful to have had the opportunity to work with such a remarkable group of individuals as the staff at FDA and will do my best to continue to advance public health in the future.

Sincerely,

Peter Marks

Peter Marks, MD, PhD

50 YEARS AdvaMed The Medtech Association

Login

← Press Releases

AdvaMed® Statement on Reports of Significant FDA Job Cuts

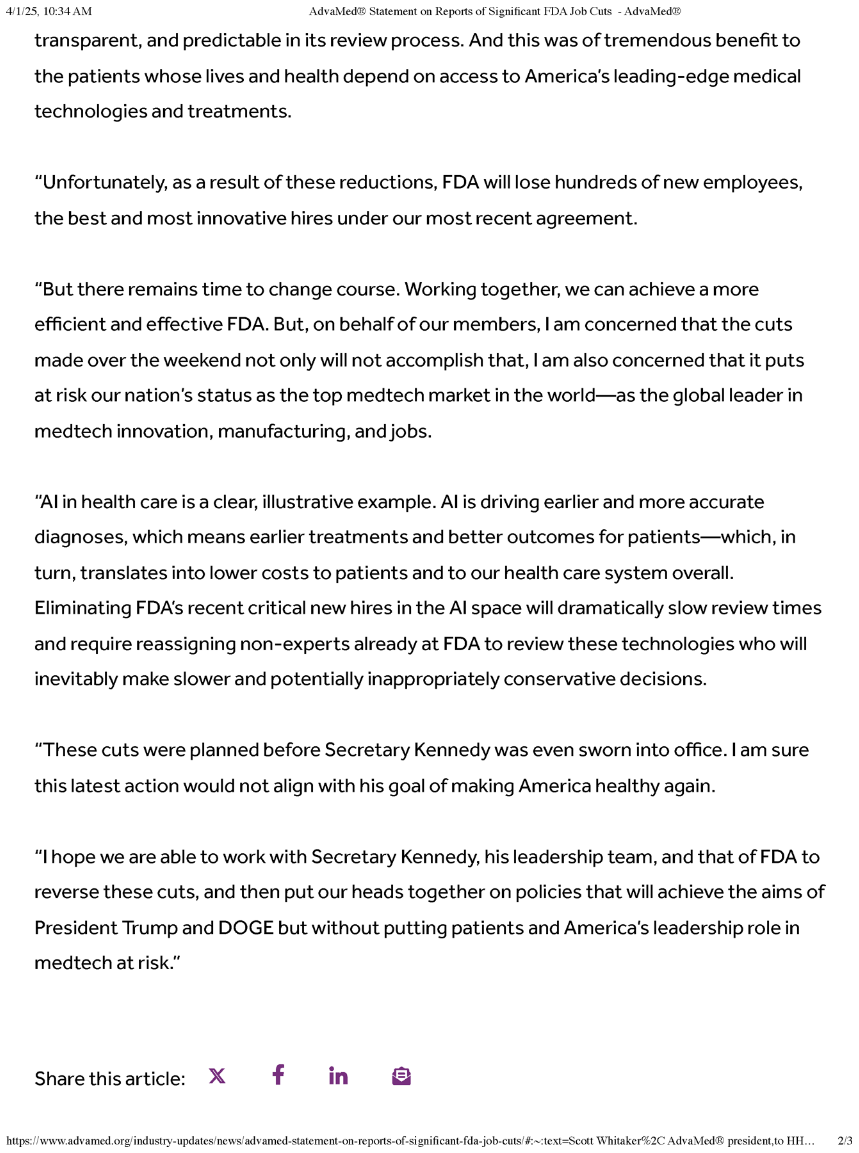
February 18, 2025

Washington, D.C. – AdvaMed®, the Medtech Association, is the world's largest trade association representing medtech companies, ranging from multinational corporations to the smallest businesses and startups. The health care system relies on FDA regulation of medtech. The FDA determines whether a medtech device may be marketed to patients and providers. A user fee agreement between FDA and medtech companies, authorized by Congress, funds part of the regulatory setup. Scott Whitaker, AdvaMed® president and CEO, made the following **statement** on LinkedIn on news reports of significant FDA job cuts.

"Over the weekend, significant job cuts were made to FDA that could have a very negative impact on patient care in this country. Today, I sent a letter to HHS outlining our concerns.

"We understand and support the administration's overall goal to be more efficient with the taxpayer dollar. Our concern is that this round of cuts to FDA staff runs counter to that shared goal.

"Device review times were already too long, though they were improving as the result of our latest user-fee agreement. FDA was already struggling to keep pace with our industry's tens of thousands of new medical technology applications every year, all of which are intended to improve the lives of patients in this country. And in this regard FDA was improving as well (and also due to our latest user-fee agreement). That agreement, for the first time ever, created private sector-like incentives for FDA to be more efficient,



4/1/25, 10:34 AM AdvaMed® Statement on Reports of Significant FDA Job Cuts - AdvaMed®

transparent, and predictable in its review process. And this was of tremendous benefit to the patients whose lives and health depend on access to America's leading-edge medical technologies and treatments.

"Unfortunately, as a result of these reductions, FDA will lose hundreds of new employees, the best and most innovative hires under our most recent agreement.

"But there remains time to change course. Working together, we can achieve a more efficient and effective FDA. But, on behalf of our members, I am concerned that the cuts made over the weekend not only will not accomplish that, I am also concerned that it puts at risk our nation's status as the top medtech market in the world—as the global leader in medtech innovation, manufacturing, and jobs.

"AI in health care is a clear, illustrative example. AI is driving earlier and more accurate diagnoses, which means earlier treatments and better outcomes for patients—which, in turn, translates into lower costs to patients and to our health care system overall. Eliminating FDA's recent critical new hires in the AI space will dramatically slow review times and require reassigning non-experts already at FDA to review these technologies who will inevitably make slower and potentially inappropriately conservative decisions.

"These cuts were planned before Secretary Kennedy was even sworn into office. I am sure this latest action would not align with his goal of making America healthy again.

"I hope we are able to work with Secretary Kennedy, his leadership team, and that of FDA to reverse these cuts, and then put our heads together on policies that will achieve the aims of President Trump and DOGE but without putting patients and America's leadership role in medtech at risk."

Share this article:

https://www.advamed.org/industry-updates/news/advamed-statement-on-reports-of-significant-fda-job-cuts/#:~:text=Scott Whitaker%2C AdvaMed® president,to HH... 2/3

(QFRs) Questions For the Record
for Dr. Christian Dameff MD

House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
Hearing on "Aging Technology, Emerging Threats: Examining Cybersecurity Vulnerabilities in Legacy Medical Devices."

April 1st, 2025

The Honorable Neal P. Dunn, MD

1. Radiation therapy is a widely used and highly effective form of cancer treatment. When updated systems delivering stereotactic radiotherapy and stereotactic body radiation therapy are used to treat brain, spine, lung, prostate and pancreatic cancers, treatment outcomes are comparable and even superior to other treatment options while simultaneously saving patients and the healthcare system money. In addition to providing better outcomes, new technology radiation therapy systems can provide greater cybersecurity protections for patients and providers alike. However, providers are often slow or hesitant to adopt new technology because of misaligned payment incentives. How can CMS incentivize more providers to adopt new technology that is more cost effective, improves patient outcomes, and provides better cybersecurity protections?

Answer:

Thank you for this important question. There are several potential strategies to incentivize the adoption of more cyber-resilient technologies across healthcare delivery organizations in the United States. Two key considerations are outlined below:

1. Clinical Cybersecurity Awareness

Clinician device preferences often drive procurement decisions within hospitals, with many favoring platforms and devices they are already familiar with from training. However, transitions between devices or platforms can introduce usability challenges. To promote adoption of more secure technologies, clinicians must be equipped to consider cybersecurity risks when evaluating medical devices. Currently, there is no standardized or widely adopted educational initiative that addresses this need. Incorporating cybersecurity education into medical training—through organizations such as the Liaison Committee on Medical Education (LCME) and the Accreditation Council for Graduate Medical Education (ACGME)—could empower clinicians to make more informed, security-conscious decisions that ultimately influence safer procurement practices.

2. CMS Reimbursement Incentives

The Centers for Medicare & Medicaid Services (CMS) can play a pivotal role in accelerating the transition away from insecure, legacy medical devices. One effective approach would be to provide enhanced reimbursement to healthcare organizations that acquire and properly implement more secure, modern medical technologies. While not a perfect comparison, the 2009 HITECH Act offers a useful precedent. By providing tiered financial incentives—followed by penalties for noncompliance—the Act successfully spurred the nationwide adoption of electronic health records. A similar reimbursement model could drive rapid transformation toward a more cyber-secure healthcare ecosystem.

Intermountain Health

Mr. Erik Decker, Vice President and Chief Information
Security Officer, Intermountain Healthcare

The Honorable Russ Fulcher:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

b. Any improvements to simplify or consolidate

A few suggestions:

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

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

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

4. As former National Cyber Director Chris Inglis said:

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

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