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/

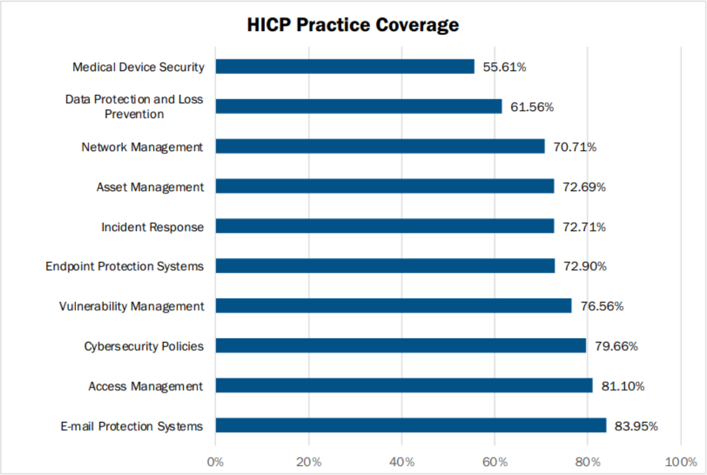
[12] https://healthsectorcouncil.org/legacy-tech-security/

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

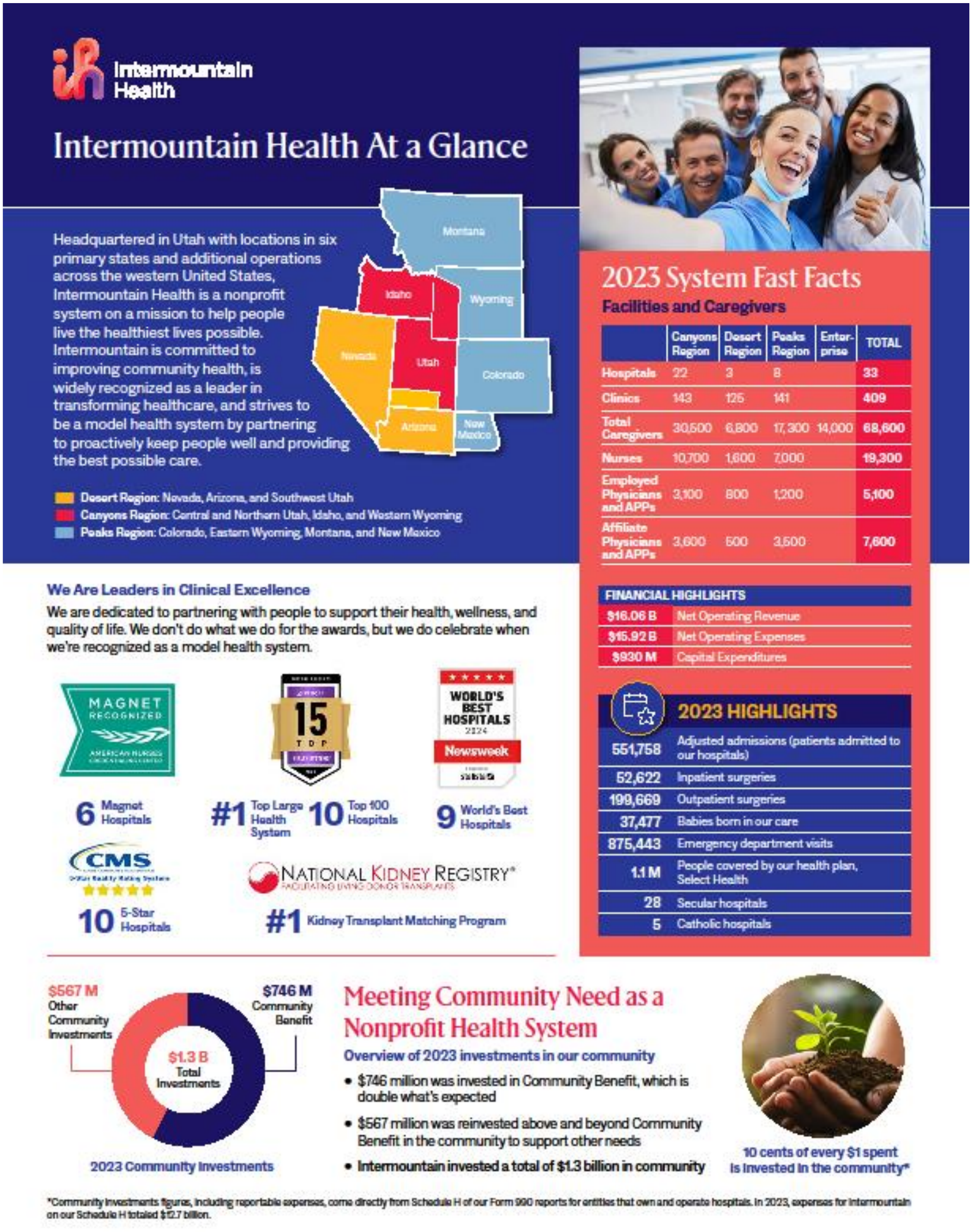
Strengthening the Bonds of the Future

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


Montana
Idaho
Wyoming
Nevada
Utah
Colorado
Arizona
New Mexico
$567 M Other Community Investments
$746 M Community Benefit
$1.3 B Total Investments

Intermountain Health

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	125	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.

MAGNET RECOGNIZED AMERICAN NURSES

15 TOP

WORLD'S BEST HOSPITALS 2024 Newsweek

6 Magnet Hospitals

#1 Top Large Health System

10 Top 100 Hospitals

9 World's Best Hospitals

CMS ★★★★★

10 5-Star Hospitals

NATIONAL KIDNEY REGISTRY® FACILITATING LIVING DONOR TRANSPLANTS

#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.