Testimony of

Erik Decker

Chairman, Cybersecurity Working Group

of the Health Sector Coordinating Council

and

Vice President, Chief Information Security Officer, Intermountain Health

on

"Preparing for and Responding to Future Public Health Security Threats"

Before the

Subcommittee on Health of the

Committee on Energy and Commerce

U.S. House of Representatives

May 11th, 2023

Summary of Testimony

Chairman Guthrie, Ranking Member Eshoo, and Members of the Subcommittee, I am Erik Decker, Chairman of the Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) and Vice President and Chief Information Security Officer for Intermountain Health. Thank you for the opportunity to speak on behalf of the Cybersecurity Working Group (CWG) of the Health Sector Coordinating Council (HSCC) on public health security threats and how this interrelates with the reauthorization of PAHPA.

As a critical infrastructure operator, and the chair of the Health Sector Coordinating Council's Cybersecurity Working Group, I believe we have reached an inflection point: our adversaries are becoming increasingly sophisticated at penetrating our cyber defenses just as we are becoming increasingly reliant on digital data and technology. We leverage digital data and technology to improve health and healthcare, to make the health workforce more productive, and to advance health equity. 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 Health and Public Health (HPH) Sector continues to be a top focus for cyber-attack. Ultimately, these threats have led to troubling potential patient safety risks and negative impacts to public health.

Thankfully, the partnership between the HPH Sector and the U.S. 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.

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

1. The current state of adversarial cyber threats and their potential for future damage
2. The current state of the HPH Sector's cyber capabilities and partnership

3. Suggestions for strengthening the HPH Sector's partnership with the U.S. Government that will better protect all of us from cyber threats.

We must continue to work in partnership, with the industry improving its capabilities across all its subsectors, and the U.S. Government improving its services to critical infrastructure, cohesion across government, supplying incentives to strengthen cyber capabilities, and where necessary, regulation.

Adversarial Threats

Over the last several decades, the HPH Sector and U.S. Government have established preparedness and resilience around biological, environmental, and man-made threats. These preparations have generally focused on kinetic or physical threats, which can damage components of our infrastructure and our ability to deliver care. They can come in the form of a hurricane causing a regional public health issue and impacting access to acute care, a national pandemic that involves overloading of the health system, and medical supply chain challenges, including an insufficient Strategic National Stockpile. Several programs have been established to help prepare the HPH Sector for these threats, such as those programs authorized under PAHPA, the Hospital Preparedness Program under HHS/ASPR, cooperative agreements under the Public Health Emergency Preparedness program, and others.

One threat that continues to be pervasive and tenacious is the cyber threat. This threat is relatively new to the HPH Sector, having materialized and actualized its kinetic damage over the last ten years. Though the HPH Sector has long established programs to protect the sensitive data stored and used within their remits, it is only relatively recently that cyber-attacks themselves have disrupted the ability to deliver care, receive mission or life critical supplies and services, or even threatening the ability to create novel medicines, vaccines, and other therapies. This inflection point is a direct result of the digitalization and innovation of new technology into the health sector. Elements of this began in the early 2000s with the explosion of the Internet, the introduction of new and connected medical technology, the use of

automation within manufacturing facilities for the development of medicines and vaccines, and the adoption of Electronic Medical Records (EMRs) and other clinical applications for the purposes of diagnosing and treating disease.

These technological advances are components of a core and central purpose – to improve healthcare, wellness, and wellbeing. To achieve this, our national healthcare system has become an ecosystem of highly interconnected businesses, functions, people, and technologies. No single hospital system in the United States operates independent of partnerships. Those partnerships might materialize in the form of reciprocal agreements, service relationships with medical technologies, supply chains purchasing key medicines and therapies, consulting and service delivery agreements, environment of care connectivity, the use and delivery of connected medical devices, and hundreds or thousands of applications that run both on-premises, in the cloud, or hosted by service partners. The interconnectivity is staggering, and yet each intersection introduces a potential point of exploitation and weakness.

In the past several years criminal organizations and nation state actors have become a significant threat. In 2016, a major ransomware attack shut down a hospital system in Southern California. Though ransomware threats have been around prior to 2016, this was one of the first known cases where the malware caused a full shutdown of a hospital system itself. Another attack quickly followed shutting down a hospital in Washington D.C. In 2017 the world saw the first launch of automated and self-propagating malware called WannaCry. Within days the UK National Health System was shut down, causing a national health crisis. There were anecdotes that WannaCry had spread into US networks before it was nullified through a rather ingenious technical defense, which was discovering and activating a kill switch that was built into the malware by the adversaries.

Following quickly after WannaCry, a disruptive wiper malware called NotPetya was released into the wild. This damaging malware, which allegedly was launched by Russia against the Ukraine in 2017,

reportedly caused more than $10 billion dollars in damage to some of the world's largest firms (including U.S. healthcare companies). During the COVID-19 pandemic we saw adversaries attacking organizations as they attempted to safely manage the spread of the virus. Adversaries tried to capitalize on the pandemic in several ways. Naturally they used the pandemic to further social engineering attacks which lead to more data theft and disruptions. We also witnessed the use of misinformation campaigns where adversaries attempted to discredit the safety and efficacy of vaccines.

These cyber-attacks were just the beginning of a new wave of threat: the ability for criminal organizations and nation state actors to leverage the interconnected and digital nature of our economy in a disruptive manner. The very foundation of our new technological paradigm has been used against us.

Given this target rich opportunity, our cyber adversaries have found it lucrative to invest in their own capabilities and establish underground markets where credentials, vulnerabilities, and 'ransomware services' are bought and sold. As our adversaries have increased their sophistication they have demonstrated the ability to inflict significant damage to the U.S, with some recent examples such as 1) the intrusion into SolarWinds in December of 2020 whereby malicious code was delivered to thousands of US companies from coast to coast, 2) the shutdown of the scheduling and payroll management system hosted by Kronos causing pay and scheduling disruptions to thousands of customers in December 2021, 3) several prominent attacks from 2020 to 2023 on U.S. Hospitals likely causing regional damage and overflow affects to emergency and acute care, and 4) an attack against the European Medicines Agency in 2021 that resulted in both a theft of intellectual property of COVID vaccines as well as the manipulation of COVID vaccine data for the sole purpose of undermining the public trust in the vaccines themselves. This latest action is a troubling new style of misinformation warfare designed to undermine the public trust in medical data itself.

The future of cyber threats is just as pernicious as the past. As the HPH Sector bolsters its cyber resilience we expect our adversaries will pivot. The potential of new cyber-attack could manifest itself in several ways, including:

- In an AI-enabled future the data models we leverage are used for making care decisions. These models will be fed not only by clinicians but also by medical technology, laboratory and imaging results, and the efficacies of drug therapies. If we are not careful, we could become vulnerable to either accidental or malicious "data poisoning" of our decision models. If actualized, harmful treatment decisions could be made causing harm to our patients and eroding the trust in the healthcare system.
- Compromising the very integrity of key records themselves, such as patient records, drug efficacy study data, or the effectiveness of medical technology, all for the sole purpose of sowing distrust in the innovation, diagnostic measure, or therapeutic.
- Attacking and disrupting specific Critical Infrastructure services that are used specifically by the HPH Sector, such as water, energy, or oil and gas, to further harm public health and trust.

Without the proper cyber foundations in place, this velocity of digital transformation could become the equivalent of driving a race car at maximum velocity without brakes.

Current State of Critical Infrastructure Partnership and Cybersecurity Capabilities

Public-private partnership within the HPH Sector is key and critical to a safe future. No single organization, no matter how resourced, can be expected to stand up against the weight of a nation state adversary. The task of countering these adversaries is even more daunting for smaller hospitals that provide critical care to rural and underserved areas. The HSCC CWG is an industry leading advisory council of healthcare organizations, government agencies and advisors working in partnership under the auspices of the Department of Homeland Security (DHS) Critical Infrastructure Partnership Advisory Council (CIPAC) framework. The current membership exceeds 800 individuals representing more than 400 organizations. Our mission is 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. Or, as we call it, "cyber safety is patient safety".

The HSCC CWG was rechartered in 2018, which was preceded by the appointment of Greg Garcia as the Executive Director of the CWG. This rechartering, and with the leadership of Mr. Garcia, spearheaded a major investment and realization of the public-private partnership. In 2017 the HSCC CWG was made up of 50 organizations and only a few U.S. Government representatives. As of Q1 of 2023, the working group is strong with 409 organization members, with a total of 857 personnel representing those organizations. This includes 10 federal agencies, 3 state agencies, 2 city agencies and 2 Canadian. Direct Patient Care continues to represent the largest subsector at 39.4%, followed by Medical Materials (8.8%), Cross-Sector (8.8%), Pharmaceuticals, Laboratories, Blood (6.4%), Public Health (5.3%), Health Plans and Payers (4.6%), Government (4.2%), Health Information Technology (9.5%) and finally a set of subject mater experts called Advisors (13.2%).

The HSCC CWG allows for multiple methods to be engaged, via the website: https://healthsectorcouncil.org. Importantly, there are no membership dues to participate and CIPAC

does not permit the collection of dues. Critical Infrastructure operators are encouraged to join and participate in one of the 15 active Task Groups. Members have opportunities to either lead existing Task Groups or propose to the CWG leadership to establish new Task Groups. The CWG is supported by an Executive Committee, which are elected positions from the CWG membership representing all 7 of the HPH subsectors. The Executive Committee votes in the Chair and Vice-Chair. Each of these positions have term limits to ensure a democratic process and infusion of new ideas.

Since 2018 the HSCC has produced 21 best-practice publications to aid all 7 subsectors of Health and Public Health. With recent executive sponsorship from the HHS Deputy Secretary, the partnership between HSCC CWG and HHS has also recently accelerated. Of the 21 best-practice publications, 4 of them have been jointly branded and released between both the HPH Sector and HHS over the past two months. Those are Health Industry Cybersecurity Practices (HICP), the Hospital Cybersecurity Resiliency Landscape Analysis, the HPH Sector Cybersecurity Framework Implementation Guide and the 405(d) Knowledge on Demand education materials and training platform. These and all HSCC CWG publications are developed by diverse groups of healthcare cybersecurity experts who donate their time so that these resources can be available at no charge to anyone in the HPH Sector.

More joint publications are planned to be released later this year. Of the 17 other publications, many of the publications are jointly run between both industry and HHS, such as those related to medical technology. The FDA has been and continues to be a strong supporter of the partnership, co-leading 4 of the 17 publications.

These publications were built either in reaction to specific issues, such as the COVID-19 pandemic, or strategically determined to be a gap that needed additional support.

- The inaugural publication, and one of the core task groups demonstrating joint public-private partnership, the 405(d) Task Group, supported by the HHS 405(d) Program, has delivered three

joint publications. In 2018, the inaugural Health Industry Cybersecurity Practices (HICP) was launched, which outlines cyber hygiene stratified across small, medium and large size organizations. HICP was just recently updated by the same task group to the new version: HICP 2023. This partnership is also the mechanism by which the Hospital Cybersecurity Resiliency Initiative was organized, sponsored by the HHS Deputy Secretary. That publication, called the "Landscape Analysis", is the second joint publication under the HHS 405(d) Program which is a first ever quantitative and qualitative study of the current state of our nation's hospital cybersecurity resiliency. This is a keystone study towards understanding further technical and policy interventions to make for our nation's hospitals. In tandem with the new releases, the HHS 405(d) Program launched "Knowledge on Demand", a cybersecurity education platform on their website which provides free professionally developed built and packaged cybersecurity training on cybersecurity hygiene. Additionally, in 2021, Public Law 116-321 was passed which defined "Recognized Cybersecurity Practices" (RCPs), and specifically defined publications created under the 405(d) Program as RCPs. This new law instructs the HHS Office for Civil Rights to consider the adoption of RCPs over the prior 12 months when conducting enforcement activity. This is a great first step toward incentivizing the adoption of good cyber hygiene.

- In partnership with the FDA, the HSCC CWG is making incredible headway on addressing the current challenges with medical technology. Publications produced in the last 4 years include: Medical Device and Health IT Joint Security Plan (2019), Model Contract Language for MedTech Cybersecurity (2022), MedTech Vulnerability Communications Toolkit (2022), Health Industry Cybersecurity – Managing Legacy Technology Security (2023)
- During COVID the HSCC CWG was active at producing publications to help steer the industry through the new landscape of COVID-related cybersecurity threats. These included: Health Industry Cybersecurity Information Sharing Best Practices (2020), Health Industry Cybersecurity

Tactical Crisis Response Guide (2020), Health Sector Return-to-Work Guidance (2020), Management Checklist for Teleworking Surge During COVID-19 Response (2020), Health Industry Cybersecurity – Securing Telehealth and Telemedicine (2021), Operational Continuity Cyber Incident (2022).

- Also in 2023, a joint HPH Sector Cybersecurity Framework Implementation Guide was produced. This effort was supported and released by ASPR, in partnership with the HPH Sector. This guide aids organizations in adopting the NIST Cybersecurity Framework.
- Additional publications focused on the workforce include: the Health Industry Cybersecurity Workforce Guide (2019), and just recently a new series of professional built videos for educating clinicians on the current state of cybersecurity threats, the Cybersecurity for the Clinician Video Training Series (2023)
- Other notable publications include: 1) Publications related to best practices on sharing cybersecurity threat intelligence information Health Industry Cybersecurity Matrix of Information Sharing Organizations (2019), and Health Industry Cybersecurity Information Sharing Best Practices (2020), 2) Publications related to managing the significant challenge of third party risk Health Industry Cybersecurity Supply Chain Risk Management Guide (2019) and its subsequent update in Version 2 in 2020. Lastly, the recently produced guidance on specific considerations for the use of AI with the Health Industry Cybersecurity Artificial Intelligence Machine Learning (2023) publication

All this organization and production of content demonstrates how busy the partnership has been over the last 5 years. The 15 currently active task groups are currently working to generate new content and new products. Examples of this partnership include a new task group focusing on the cohesion between Privacy and Cybersecurity Programs and a task group focused on Public Health Cybersecurity challenges.

The level of engagement dramatically accelerated in the last year. In the month of April alone, 4 of the 21 publications were released, and 2 of them were HHS joint sealed products. This is representative of the increasing interest and support of the executive leadership of HHS as well as CISA. Several major initiatives have taken place in the last 12-18 months, including:

- A CEO White House healthcare cyber summit in June 2022. The CEOs of the HSCC CWG leadership were invited at the request of the National Cybersecurity Director, Chris Inglis, to discuss the current state of cybersecurity challenges in a cabinet level meeting with representation from the U.S. Department of Health and Human Services, the National Security Council, Department of Homeland Security, and Cybersecurity and Infrastructure Security Agency. At this meeting the group committed to investing in future cyber defenses with commitments amongst the CEOs and the senior officials to enhance the partnership.
- Strategic partnership meetings every other Friday between HPH Sector, HHS and CISA leadership. These meetings allow for strategic visioning and planning, as well as managing emergent situations such as the Ukraine-Russia conflict.

The partnership is strong with HHS, but our work is not done. We are only at the early stages of attaining our potential.

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. Our bodies have built a complicated immune system to respond to threats in such a manner. 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.

Our bodies do not require each individual antibody or white blood cell to shoulder the burden of an entire army of pathogens. Neither should we expect every organization to defend against these cyber threats independently and autonomously. We must band together, not only as the HPH Sector and HHS, but the whole of all critical infrastructure and all of the U.S. Government. The problem might seem daunting, but just like the HPH Sector responded to the COVID pandemic and every day pushes us closer to a cure for some of the world's most devasting chronic diseases, we can meet this challenge as well.

The HSCC CWG is working on improving its foundation and contemplating what "Stable Condition" for cybersecurity in the HPH Sector looks like in 2029 by running a 5-year strategic planning exercise. By the end of 2023 we will release our 5-year strategic plan. This plan contemplates the future of healthcare in the context of a) Clinical trends, b) Business Trends, c) Policy and Regulation and d) evolving Technology, such as the rise of digitization and AI. As with all strategic programs, there are elements of our foundation that we should strengthen and there are brand new capabilities we should introduce. The following is a list of potential improvements, both strategic and tactical, being contemplated as part of the HSCC CWG Strategic plan:

- The continued expansion and improvement of the HHS 405(d) Program, which is a core vehicle of the partnership with the HPH Sector and HHS. This Program, run by HHS, is the mechanism by which the first joint HSCC and HHS publication was produced and released by both the industry and the US Government: Health Industry Cybersecurity Practices (2018). This publication was the cornerstone publication to advising on cyber hygiene for the HPH Sector. It was called for in the Cybersecurity Act of 2015, under Section 405(d): Aligning Cybersecurity Practices for Healthcare. HHS over the past several years has not only built an entire program to support these joint efforts, but also a dedicated HPH outreach and engagement platform by which they are consistently engaging with the sector and providing cyber hygiene awareness resources and tools. It is a shining example of how Critical Infrastructure partnership can produce consensus-based advice, with over 150 members of the HSCC CWG working to develop the original document. This Program is also the mechanism by which the *Hospital Cybersecurity Resiliency Initiative* was organized. Sponsored by the HHS Deputy Secretary we produced the "Landscape Analysis", which analyzed the current state of US hospital cybersecurity resiliency. The reach of the Program is strong, with more than 600,000 hits to the website and 17,000+ downloads of HICP and the Landscape Analysis in the first two weeks of its launch. We also received 2600+ new subscribers, 1200+ new social media followers and 10,000+ downloads of the 25 total 405(d) Products this year alone. In contrast, since 2019 of all the HSCC CWG 21 publications and products, we have received only 230,000 website hits and 12,000 downloads. The difference between these two demonstrates the scale and market penetration that the whole of HHS operates, and the additional support and membership needed by the HSCC. Further partnership and endorsement with HHS can improve the HSCC membership.
- Continued partnership and cohesion between CISA, HHS and the HPH Sector is also underway. CISA produces many useful tools and services, and they are experts in the cybersecurity

discipline. With the upcoming rulemaking to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2021 (CIRCIA), we are excited to work through the specifics of how we will incorporate the threat intelligence received from all 16 Critical Infrastructure sectors and consume them into our proactive defenses. This is truly a mechanism to achieving shared defense. However, these programs must be accomplished with cohesion and partnership between HHS, CISA and the HPH Sector. HHS is the HPH Sector's Risk Management Agency, our forward-facing agency that the sector knows. Our future engagement needs to leverage HHS as our 'gateway' to all the products and services offered by the U.S. Government; anything outside of this will be confusing for those who are not well versed with engaging with our federal government.

- Cohesion within the HPH Sector and our designated Sector Risk Management Agency (SRMA), which is HHS. Cybersecurity is one threat of many, as contemplated earlier in this testimony. However, the challenges associated with cybersecurity are unique and different from managing biological or environmental threats. It takes a different discipline, expertise and sets of resources. We continue recent momentum on driving increased cohesion and coordination across all the HHS Operating and Staff Divisions. We have seen tremendous progress here despite minimal resources; continued support for SRMA resources and investment in HHS as the SRMA would absolutely be beneficial. Ultimately, we must capitalize on the emerging sponsorship from the CEO White House Cybersecurity summit in 2022 to take our partnership to the next level.
- The U.S. Government must do better at delivering non-attributed threat intelligence from all agencies of the government, packaging and delivering actionable intelligence to all 16 Critical Infrastructure sectors. Multiple sources of threat intelligence exist across the U.S. Government. The three agencies with which the HPH Sector interfaces most frequently are HHS, CISA and the

FBI. We need to improve this partnership to deliver more timely intelligence. The concerns around attribution of classified information are understood, however the source of intelligence is not what is needed by the HPH Sector, rather the relevant Indicators of Compromise (IOCs) and Tactics, Techniques and Procedures (TTPs). These need to be specific, accurate, concise, targeted and delivered at machine speed for us to stay abreast of the threat actions. Several programs exist today supported by CISA to deliver some elements of this intelligence, but only pieces of it are highly curated and only certain organizations have access to it.

- Tailor a healthcare liaison classified information sharing program with industry-designated representatives of the HPH Sector, CISA, the Health Sector Cybersecurity Coordination Center (HC3), and law enforcement agencies, so that the HPH representatives can provide consideration and feedback to federal threat analysts on what is most relevant and actionable to the HPH Sector.
- While there has been great success within the HPH Sector on growth over the last 5 years, the HSCC CWG still only represents a small percentage of the total healthcare organizations in the United States. Those who participate are aware of our cybersecurity challenges and are trying to be a part of the solution. Many entities do not participate and do not understand the full nature of the problem. We have a lot of work to do. HHS could help elevate the outreach and importance of membership by reaching out to CEOs and other senior healthcare executives across the nation. Similarly, the CEOs of existing HPH Sector participants can also evangelize and encourage their peers to become members. Also, celebrity spokespeople could be considered; for example, those willing to speak publicly about their child's hospitalization could stress the importance of guarding against cyber attacks so hospital services remain available 24/7.
- Incentivization and reimbursement to those parts of the HPH Sector that are under resourced and incapable of achieving even basic cyber hygiene would benefit the entire HPH Sector. Given

the whole of the HPH is made up of different subsectors, some of these subsectors work within comfortable profit margins whereas others do not. For example, the Medical Technology and Pharmaceutical organizations tend to be well resourced for-profit organizations with high EBITDA ratios, but many Direct Care organizations, such as hospitals, are not-for-profit organizations operating off razor thin margins of 1-2% (if they are profitable at all). Many of the smaller organizations, such as critical access hospitals and rural hospitals continue to struggle keeping their doors open. This often means that they lack the financial wherewithal to implement cyber defenses and are left hoping they do not become victims. Incentives need to account for the equity disparity of the HPH Sector.

- Assist under resourced health systems improve their situational cybersecurity defenses by joining information and sharing and analysis centers (ISACs) like the Health-ISAC. The ISACs allow for deliberation and sharing of cyber threat IOCs, TTPs and other discussion points amongst the critical infrastructure sectors. The ISACs are also a perfect connection point of sharing "up and down" with the U.S. Government. By getting more representation into the ISACs we will be able to have broader reach across every critical infrastructure sector.
- Establish a Federal-sponsored Incident Response support program, which assists organizations experiencing significant and disruptive cyber-attacks. This program can take on elements of breach and forensic response through a national retainer with key cybersecurity firms, as well as creating a FEMA-style program to surge clinical capability into hospitals shut down due to cyber-attacks. This program could be modelled off the National Emergency Tele-Critical Care Network program from the Telemedicine & Advanced Technology Research Center (TATRC).
- Future improvements must consider cross-sector engagement across all 16 Critical Infrastructure sectors, rather than establishing defenses inside each sector itself. The sectors are reliant upon one another. For example, the HPH Sector is critically reliant on the Water and

Energy sectors, whereby catastrophic damage to them could cause significant complications to public health and patient safety. As such, our defenses should stretch across all appropriate sectors

- Further harmonization of cyber incident reporting requirements should be evaluated. For the for-profit companies in our sector, the SEC will require material reporting of cyber incidents within 72 hours. CISA will also require reporting of cyber incidents impacting critical infrastructure within 48 hours. The HHS Office for Civil Rights (OCR) requires HIPAA-covered entities to report privacy breaches pursuant to HITECH no later than 60 days after discovery of the breach. A full 47 states have their own independent reporting requirements. Precious time and resources are spent navigating the reporting obligations which takes away from the larger goal: we should be sharing in a streamlined manner amongst our community the cyber threat and vulnerability issues we manage so the whole of the HPH Sector can be protected.

Closing Thoughts

Thank you for the opportunity to provide my perspective and represent the HPH Sector 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 public health. 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 Patient safety.

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.