HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership

Testimony of

Greg Garcia

Executive Director

of the

Healthcare and Public Health Sector Coordinating Council

Cybersecurity Working Group

Before the

United States Senate

Committee on Homeland Security and Government Affairs

March 16, 2023

Introduction

Chairman Peters, Ranking Member Paul, 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 350 healthcare organizations and government agencies working in partnership under the auspices of the DHS Critical Infrastructure Partnership Advisory Council (CIPAC) framework and Presidential Policy Directive 21. 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.

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, as the HSCC is indeed conducting a "checkup on the cybersecurity risks to the healthcare sector." Today, I will cover four areas that will help inform both the diagnosis and prescription for healthcare cybersecurity:

First, I will provide a brief overview of recent trends in cyber threats, vulnerabilities and incidents facing the healthcare sector;

Second, I will offer some observations about how the healthcare industry is changing in ways that could aggravate those threats and related incidents;

Third, I will review how the industry has organized and partnered with the government over the past five years to address these concerns and how we are mobilizing to get ahead of them over the next five years; and

Fourth, I will offer examples of how our government agencies and Congress may support the health industry's efforts to augment our security and resilience against ongoing cyber threats.

Cyber Threats, Vulnerabilities and Incidents

The "healthcare cybersecurity" reference 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.

Today, because of the rise in digital healthcare, technological advances, and the efficiencies of connecting devices and data, the cyber "attack surface" in healthcare – and the adversaries intent on exploiting them – have expanded.

Threat actors are motivated to attack, including monetizing ransomware and stolen health data; operational disruption; intellectual property theft; revenge; or geopolitical leverage. The focus has traditionally been on data and privacy, but if healthcare delivery organizations (HDOs) or their suppliers cannot deliver services, as has been seen in numerous ransomware attacks, or data is manipulated or destroyed, patient lives can be at risk.

Incidents and Impacts

Data Breaches

The Office for Civil Rights in the Department of Health and Human Services, which enforces Health Insurance Portability and Accountability Act (HIPAA) data breach reporting, reported:

- Healthcare data breaches of 500 or more records (name, address, medical and financial records) increased from 329 to 715 between 2017 and 2021, with the number of individuals affected ranging between 20 million and 50 million;
- In 2022, there were 707 data breaches, more than half of which occurred against third party service providers that handle protected health information; and
- Of the 52 million data records exposed in 2022, 43.9 or 84% were caused by hacking.

And according to an IBM Cost of a Data Breach 2022 report:

- For the 12th consecutive year, the Health Provider and Pharmaceutical subsectors recorded the first and third highest costs for data breaches, followed by Financial Services, Technology and Energy;

- The average breach cost in healthcare increased by nearly $1M and is now $10.1M; and
- Costs overall have increased by over 40% in the last two years.

Ransomware and other disruptive cyberattacks

Widely reported incidents experienced over the past few years by health systems such as Scripps Health, University of Vermont Health Network, and CommonSpirit 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;
- Radiation and other treatments for cancer patients, including surgery, delayed;
- Medical records about prescriptions, diagnoses, and therapies become inaccessible and some, permanently lost;
- 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;
- Staff furloughed; 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:

- Damaged reputation
- Lost patient trust
- Lawsuits
- Regulatory penalties
- Strained employee morale and burnout, and
- Reduced stock value.

Common Methods of Attack

The Health Information Sharing and Analysis Center (Health-ISAC) – the operational defense collective of the health sector - surveyed its members asking them to rank order the Top 5 "*greatest cybersecurity concerns*" facing their organizations for both 2021 and 2022. The survey included cyber and non-cyber executives, multiple healthcare subsectors (e.g., Providers, Pharmaceutical Manufacturers, Payers, Medical Device Manufacturers, and Health Information Technology), and healthcare organizations of varying sizes and budgets. The Top 5 threats, which were the same for both 2021 and 2022 were:

1. Ransomware Deployment, by which the adversary can inject networks with malware that encrypts - or renders inoperable - networked devices and software applications

and data and demands a ransom in exchange for returning the data and operations to the health provider;

2. Phishing/Spear-Phishing Attacks, by which the adversary sends bogus emails that trick employees, clinicians, or influential senior executives into divulging information, clicking on malicious links, or opening corrupted attachments that release malware into the network;
3. Third-Party/Partner Breach, by which business partners or third party software that support clinical or business operations become infected, in turn infecting networked clinical and business operations of the healthcare entity;
4. Data Breach, which involves the theft and exposure of protected health information that can include name, address, social security number, insurance and financial information, and patient data; and
5. Insider Threat, by which employees inadvertently, carelessly, or maliciously allow malware or other adversarial actions into the health system network.

The Related Scourge of Misinformation and Disinformation

Pandemic-themed disinformation and misinformation tactics in phishing and other social engineering subterfuge often resulted over the past three years of the pandemic in compromised systems, stolen data and identity theft, resulting in degradation of trust in the industry. Many of the peddlers of spam and malware have engaged in or allowed their tools to be used to disseminate deliberately false information. While misinformation might cause

discomfort and arguments in other areas, disinformation in the healthcare area could lead to the loss of lives. COVID was a sad example in which even the most vulnerable citizens succumbed to misinformation and paid a tragic price.

Current and Future Dynamics in the Healthcare System

The health sector is highly interconnected:

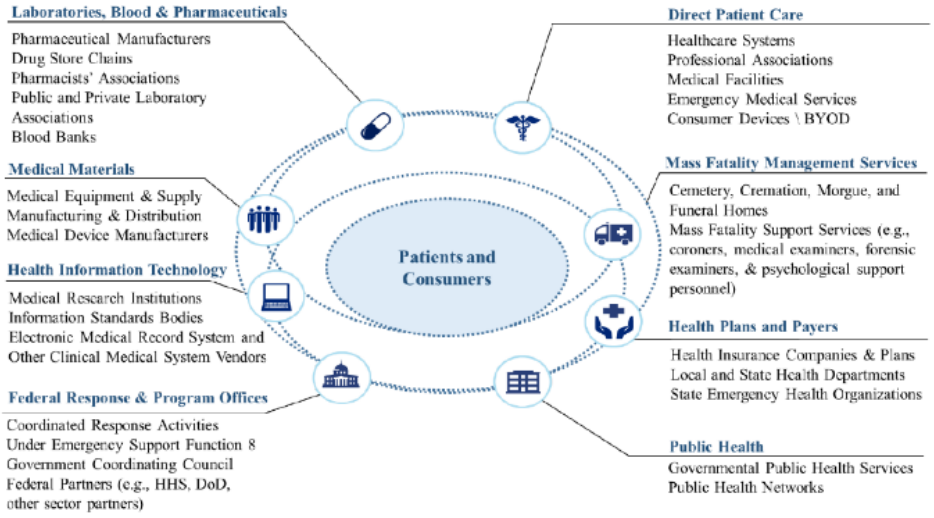
- Unlike in other sectors, healthcare data must be portable. Sensitive patient information must move between various medical providers, pharmacies, diagnostic facilities, and payers to facilitate proper patient care and payment for those services;
- Many healthcare facilities, such as hospitals, operate 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 often have unencrypted hard drives or common passwords set by the manufacturer that cannot be changed;
- Accompanying this range of manufacturers are many differing support models, timing for developing patches and methods for their deployment. This adds time, cost and complexity to hospitals' ability to manage effectively;

- Hospitals utilize many devices with outdated operating systems that are not supported by the manufacturers. Expensive equipment such as Magnetic Resonance Imaging (MRI) machines are not easily replaced as they run 24 hours a day, seven days a week, 365 days a year. Implementing compensating controls, or taking them offline for patches, updates or replacements is complicated. Further complicating HDO replacement programs are budget constraints and small operating margins;
- When supply chains are tightened or non-existent for various reasons, or pandemics or natural or man-made regional disasters occur, stretched supplies and staff become additional factors; and
- Coupled with a diverse base within the sector, complex siloed departments, a lack of skilled cyber staff, cyber security situational awareness, knowledge and training for the medical staff and CEO and Board levels, and lack of cyber security strategy including a risk management approach, the health, and public health sector face an enormous challenge.

HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership

The connected healthcare ecosystem

Figure 2 Health Care Ecosystem



An Organized Partnered Response

Policy Foundation. U.S. national policy (Presidential Decision Directive 63, Homeland Security Presidential Directive 7, Presidential Policy Directive 21) designates 16 essential industries as "critical infrastructure," including healthcare, financial services, energy, telecommunications, water, transportation, and more. These critical sectors are represented by industry-organized "sector coordinating councils (SCCs)." These SCCs and their government counterparts form a national public-private partnership coordinated overall by the U.S. Department of Homeland Security through the National Infrastructure Protection Plan (NIPP).

The Sector Coordinating Councils (SCCs) are self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities.

The SCCs coordinate and collaborate with sector risk management agencies (SRMAs) and related Government Coordinating Councils (GCCs) to address the entire range of critical infrastructure security and resilience policies and efforts for that sector.

SCCs serve as the sector's voice and facilitate the government's collaboration with the sector for critical infrastructure security and resilience activities. In addition, the SCCs are encouraged to establish voluntary practices to ensure that sector perspectives are included. Other primary functions of an SCC may include the following:

- Serve as a strategic communications and coordination mechanism between owners, operators, trade associations, suppliers, and the government during emerging threats or response and recovery operations, as determined by the sector;
- Identify, implement, and support appropriate information-sharing capabilities and mechanisms in sectors where no information-sharing structure exists;
- Encourage representative sector membership;
- Participate in planning efforts with designated SRMAs (the designated SRMA for healthcare is the U.S. Department of Health and Human Services) related to longer term strategic plans;
- Facilitate inclusive organization and coordination of the sector's policy development regarding critical infrastructure security and resilience planning and preparedness,

exercises and training, public awareness, and associated implementation activities and requirements;

- Identify, develop, and share information with the sector (both public and private sector members) concerning effective cybersecurity practices, such as cybersecurity working groups, risk assessments, strategies, and plans; and
- Provide input to the government on sector research and development efforts and requirements.

For the government's part, SRMAs have enumerated partnership responsibilities promulgated under §9002 of the FY 2021 National Defense Authorization Act, to include:

1. Provide specialized sector-specific expertise to Critical Infrastructure (CI) owners and operators in the sector or subsector;
2. Support the sector or subsector's programs and associated activities;
3. Carry out responsibilities in coordination with DHS, other relevant departments and agencies, independent regulatory agencies, and state local tribal and territorial entities as appropriate, and in collaboration with the sector's CI owners and operators; and
4. Utilize specialized expertise in the sector to support sector risk management in coordination with the CISA Director, including establishing and carrying out programs to help owners and operators identify, understand, and mitigate threats, vulnerabilities, and risks to their systems and assets, recommending security measures to mitigate risks,

assessing sector risk, coordinating with the sector, facilitating information sharing, and supporting incident management.

Critical Infrastructure Partnership Advisory Council Framework. Critical infrastructure SCC-GCC partnerships operate under a CISA-coordinated framework called "*Critical Infrastructure Partnership Advisory Council (CIPAC)"* which exempts ongoing SCC-GCC engagements involving planning and decision making from standard public disclosure rules associated with federal advisory committees under the Federal Advisory Committee Act. This is due to the imperative of protecting sensitive critical infrastructure threat, vulnerability, and mitigation information from public disclosure that could encourage the malicious targeting of data and operations and jeopardize public safety and economic and national security.

Healthcare and Public Health Sector Coordinating Council Cybersecurity Working Group. The HSCC serves as an advisory council to the sector, HHS, CISA, and other government agencies, with a formally-designated critical infrastructure protection function distinct from the advocacy and member services roles of traditional industry associations. The HSCC, Health-ISAC, HHS, FDA, and CISA work jointly to identify and mitigate systemic threats to critical healthcare infrastructure, such as pandemics, major weather events, terrorism, active shooters, and cyber-attacks. The mission is to identify cyber and physical risks to the security and resiliency of the sector, develop guidance and policies for mitigating those risks, and facilitate threat preparedness and incident response.

The HSCC Cybersecurity Working Group is a volunteer council of ~380-organizations that operate under a charter-based governance structure with an elected Chair, Vice Chair and Executive Committee. Membership is open to any organization that is a) a covered entity or business associate under HIPAA; b) a health plan or payer; c) regulated by FDA as a medical device or pharmaceutical company; d) a health IT company subject to health data interoperability rules HHS Office of the National Coordinator; e) a public health organization and f) any healthcare industry association or professional society. A small allotment of an "Advisor" members – consulting, law, and security companies - is permitted to participate and support CWG initiatives pro bono.

When working with our government partners, the industry-led Cybersecurity Working Group becomes the *Joint* Cybersecurity Working Group, which identifies and develops preparedness measures against cybersecurity threats to the security and resiliency of the healthcare sector.

The HSCC Cybersecurity Working Group is currently organized into 15 function-specific, outcome-oriented task groups composed of 30 to 130 organizations across the health industry spectrum that meet regularly to develop best-practices for various healthcare cybersecurity disciplines. These disciplines include health provider cybersecurity hygiene; supply chain cyber risk management; workforce development; incident response; and medical technology security, among many others.

Last week the Cybersecurity Working Group published its 17th best-practice guidance since 2019, this one guiding healthcare organizations on how best to implement the widely recognized NIST Cybersecurity Framework. This was our second "Joint Seal" publication in partnership with HHS – a compelling indication of the importance of collaboration between industry and government, on the principle that market forces alone cannot solve our cybersecurity challenges, and regulation cannot solve those challenges. This publication also acknowledges the imperative of critical infrastructure protection articulated in the recent publication of the President's National Cybersecurity Strategy. The NIST Cybersecurity Framework was developed principally as a cybersecurity management tool for critical infrastructure industries, so our Healthcare Implementation Guide for the NIST CSF specifically addresses that imperative.

Our first joint seal publication in 2019 was the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients, which was the result of an HHS-industry partnership created by Congress in Section 405(d) of the 2015 Cybersecurity Information Sharing Act. Now four years after its publication, we have updated the HICP resource to reflect evolving threats and deterrent capabilities, which will be published jointly in the coming weeks as "HICP 2023."

And on March 1, the HSCC published a long-awaited resource laying out how medical device manufacturers and health delivery organizations can share the responsibility for managing the

cybersecurity of medical devices as they age in the clinical environment beyond manufacture or software support and patch ability. This document, more than two years in negotiation between major hospitals and medical technology manufacturers, with assistance and support from FDA, exemplified the spirit of shared cybersecurity responsibility for patient safety that is the cornerstone principle of member engagement in the HSCC Cybersecurity Working Group.

Finally, this week and over the next several weeks, we will roll out a dynamic resource to address the issue of the "insider threat" discussed earlier, with the release of an 8-part video training series – available now on YouTube called "Cybersecurity for the Clinician". This short series totaling 50 minutes will help clinicians – doctors, nurses, medical students, support staff, and many others understand the importance of helping to secure their small part of cyberspace and that it is not just the job of IT security teams. Again, accessible to anyone and any institution, this educational tool will offer continuing education credit as an incentive to click the play button and improve cybersecurity awareness and protection.

The resources mentioned above and all others we produce – by the sector for the sector - are offered as a public service free to sector stakeholders and the public via our website https://healthsectorcouncil.org/hscc-publications. Some additional publications include: *Operational Continuity after Cyber Incident; Securing Telehealth and Telemedicine; Model Contract Language for Medtech Cybersecurity; Medtech Vulnerability Communications Toolkit; Supply Chain Cybersecurity Toolkit; and Information Sharing Best Practices*. We encourage and

expect all healthcare entities among the subsectors to review these tools and implement any and all elements as appropriate into their enterprise cybersecurity programs so that collectively the sector will be prepared before, during, and after the inevitable cyber incident.

It is important to note that many of these HSCC CWG publications directly address the many important recommendations contained in the 2017 report of the Health Care Industry Cybersecurity (HCIC) Task Force, which was established by Congress in Section 405(c) of 2015 Cybersecurity Information Sharing Act and was composed of industry and government experts in healthcare and cybersecurity. The HCIC Task Force Report characterized the healthcare industry's cybersecurity preparedness as being in "critical condition." It recommended a total of 15 action items that the industry and government needed to address to raise the level of cybersecurity preparedness in the sector. Those many HCIC Task Force recommendations motivated the functional CWG task group structure, which served as the circulatory system of the council and produced our many publications. We believe and urge that broad sector-wide implementation of those scalable practices will eventually raise the sector's preparedness diagnosis to "stable."

But in the business of cybersecurity, we are never done, only better. That is why the HSCC and HHS are embarking this year on a review of how we have addressed those recommendations over the past five years, how the healthcare industry will evolve over the next five years, what associated cybersecurity challenges will be presented to us by those trends, and how we should

collectively prepare, in industry and government. Around this time next year, we expect to have a strategy to share that follows up on the HCIC Task Force report and builds on it with forward-looking assessments and measures of improvement among sector objectives.

Finally, it is important to recognize that the engagement of health sector entities to join forces against evolving cyber threats has broadened and deepened through a membership increase in the Cybersecurity Working Group from 50 organizations in 2017 to 380 today, or a 660% increase. Likewise, the Health-ISAC membership has increased by 85% since 2015, now representing more than 70% of healthcare's GDP, with 8500 member personnel sharing information around the world. Collectively, we are motivated by the existential principles that a) Cyber safety is patient safety and b) as former National Cyber Director Chris Inglis aptly articulated, "They have to beat all of us to beat one of us."

Government Action on Healthcare Cybersecurity

The following section provides: 1) a brief overview of policy actions over recent years aimed specifically at healthcare cybersecurity and 2) an overview of options for government programs, incentives, and direct support for healthcare cybersecurity that industry stakeholders have been to discuss as possible recommendations beyond simply mandating technical controls.

Policy Developments

The following partial list of legislative, regulatory or executive actions taken over the past 2-3 years illustrates the range of potential policy shifts that healthcare organizations may consider

as part of their cyber and enterprise risk management strategies. Likewise, this overview may stimulate discussion between industry and government partners about how to synthesize disparate initiatives into a coherent national critical infrastructure protection strategy.

- **Omnibus Appropriations Act Section 3305,** p. 1374 (December 2022): requires medical device manufacturers to ensure that their devices meet select minimum cybersecurity requirements, supported by device manufacturers and health delivery organizations;
- **National Cybersecurity Strategy, The White House** (March 2023): with an emphasis on protection of and minimum controls for critical infrastructure industries
- **Policy options paper "Cybersecurity is Patient Safety"** released by Senator Mark Warner (D-VA) (November 2022)
- **Deputy National Security Advisor public comments** (October 2022) that HHS "is beginning to work with partners at hospitals to put in place minimum cybersecurity guidelines, and then further work upcoming thereafter on devices and broader health care as well."
- **Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)** (March 2022): Require (p. 127) critical infrastructure owners and operators to report to the Cybersecurity and Infrastructure Security Agency within 72 hours of a substantial cyberattack or within 24 hours of a ransomware payment. Rulemaking process will take up to 3.5 years.
- **S. 3904 Healthcare Cybersecurity Act of 2022** (March 2022): - proposes closer collaboration between the Department of Health and Human Services and the

Cybersecurity and Infrastructure Security Agency, with the goal of strengthening cybersecurity in the health and public health sectors.

- **Securities and Exchange Commission** **proposed rules** (March 2022) aimed at bolstering the cybersecurity-related disclosures of regulated public companies that would require covered public companies to, among other things:
    - Report material cybersecurity incidents on Form 8-K within four business days of a materiality determination.
    - Routinely update investors on such incidents in quarterly and annual reports.
    - Analyze whether individually immaterial cybersecurity incidents are material in the aggregate and report those in quarterly and annual reports.
    - Make periodic disclosures regarding the company's cyber-related risk management policies and procedures.
    - Periodically disclose cyber-related governance information, including the board's oversight and management's implementation of cyber-related risk management policies and procedures.
    - Make periodic disclosures regarding board-level expertise in cybersecurity.
- **Federal Trade Commission** **policy statement** (September 2021) directing health apps and connected device companies to comply with the Health Breach Notification Rule. Under the Rule's requirements, vendors of personal health records ("PHR") and PHR-related entities must notify U.S. consumers and the FTC, and, in some cases, the media,

if there has been a breach of unsecured identifiable health information or face civil penalties for violations. The Rule also covers service providers to these entities.

- Class action lawsuits (June 2021) against Scripps Health in State and Fed Courts re ransomware effect on violation of California Confidentiality of Medical Information Act, Federal Trade Commission unfair trade practice regulations and the HIPAA privacy and security rules.
- Government Accountability Office report (June 2021) on the need for enhanced HHS Industry Partnership responsibilities.
- HHS OIG Report on Lack of CMS Cybersecurity Oversight of Networked Medical Devices in Hospitals (June 2021).
- Executive 14028 Order on Improving the Nation's Cybersecurity (May 2021): Section 4 encompasses medical technology security by specifying procurement requirements for Software Bills of Materials and agency guidance on purchasing systems with software defined as "critical software" for purposes of ensuring appropriate security before purchasing or deploying.
- P.L. 116-321 (HR 7898) HITECH Act Amendment (January 2021) requires OCR to consider mitigating fines and audit during a data breach enforcement if it determines that a breached entity has implemented recognized cybersecurity practices, such as NIST CSF and 405(d) Health Industry Cybersecurity Practices over the previous year.
- January 1, 2021: FY '21 NDAA Section 9002 (p. 3383) – which codified Sector-Specific Agencies (SSAs), previously defined in Presidential Policy Directive 21 (PPD-21), as Sector

Risk Management Agencies (SRMAs), and defined how DHS and SRMAs should work with each other to protect critical infrastructure.

- Cybersecurity Act of 2015 (pp. 104-108): §405c directed HHS to establish the Health Care Industry Cybersecurity Task Force and §405d directed HHS to convene an industry partnership program that eventually joined the HSCC Cybersecurity Working Group and produced the Health Industry Cybersecurity Practices.

Potential Government Support Programs

The following compilation of programmatic options have been or may be considered as potential recommendations for HHS, CISA, Congress or other Federal agencies to support healthcare cybersecurity. If designed, structured and implemented according to appropriate rulemaking or statutory authorities, these concepts could help reduce risk across the sector through incentive- or grant-based financial assistance and operational support to under-resourced health systems, particularly critical access and rural health providers.

Joint Preparedness Collaboration

- Augment the HHS 405(d) program. Resourced by HHS as a public-private partnership initiative codified by CISA 2015, 405(d) has a successful track record of partnership with industry. This model should continue with consideration for how it may be enhanced with continued industry-driven leadership;
- Healthcare Cybersecurity Workforce Development Program - HHS can administer a workforce development and cyber training program with assistance from NIST's

National Initiative for Cybersecurity Education (NICE). Elements of this program could include access to free cyber training, assistance to providers under a Regional Extension Centers model, and student loan forgiveness programs modeled after physician loan forgiveness programs or the National Science Foundation's CyberCorps(R) Scholarship for Service (SFS) program. This program provides a full scholarship plus stipend for undergraduate and master's degrees in cybersecurity and requires two years of government service.

Financial Support and Incentives

- CMS reimbursement incentives: Similar to the cybersecurity investment incentive created in the HITECH Act amendment in PL 116-321, health systems may indicate implementation NIST CSF, HICP or other consensus-based, voluntary cybersecurity frameworks for a higher reimbursement;
- HHS grant programs to help under resourced health systems improve situational awareness by joining the Health-ISAC or other information and sharing and analysis organizations;
- Expand FCC Health Connect Fund of the Universal Service Administrative Company (USAC) from WAN/Core Network investment to network and application cybersecurity;
- Immediate One-Time Funding for Baseline Security Implementation for health systems under a certain threshold of current cybersecurity investment, tied to implementation of specific cybersecurity control frameworks such as NIST CSF and HICP;

- "Cash for Clunkers" for legacy hardware replacement, modeled after the program for consumers to replace used automobiles that do not meet current emissions standards. When coupled with FDA authorities to ensure medical devices have met pre-market security requirements this program would provide a mechanism for HDOs to replace legacy and insecure technology.

Threat and Vulnerability Sharing

- Boost funding for HHS Health Sector Cyber Coordination Center (HC3) to be a primary knowledge sharing and analysis resource within HHS to support healthcare cybersecurity in coordination with CISA;
- Continue development of innovative CISA support programs, such as the Automated Indicator Sharing (AIS) program or Cybersecurity Information Sharing and Collaboration Program (CISCP), that can be tailored, in close consultation with HHS, to healthcare entities;
- Timely and actionable government sharing of cyber threat and incident information is frequently inadequate for private sector needs. When developing threat and remediation advisories for the health sector, CISA, HHS and law enforcement should as a matter of protocol consult ahead of publication with designated industry sector leaders with credible – and as appropriate, global - threat intelligence and analysis that can be compared and reconciled with government intelligence. This would ensure that both industry and government leaders are generally aligned before publication to the

broader community about the accuracy of the intelligence, its relevance to and impact on the sector, and appropriate remediation procedures;

- Tailor a healthcare liaison classified information sharing program with industry-designated representatives of the HPH Sector, CISA, HC3, and other 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 Sector;
- CISA should clearly articulate and rapidly-deliver actionable intelligence when implementing its cyber incident reporting collection and analysis authorities under CIRCIA 2022, as summarized in the previous section. Implementation should include consideration of waivers from victim reporting requirements while the incident response is underway in the early stages of discovery and operational triage;
- Protect health delivery organizations from class action lawsuits if they can demonstrate they implement NIST CSF, HICP, or other recognized cybersecurity practices and voluntarily share information about a critical cybersecurity incident with Health-ISAC, CISA, HHS/HC3, FBI, and/or state regulators. This could incentivize more robust adoption and implementation of security controls, promote voluntary information sharing, and protect against disclosure of sensitive incident information being used against the hospital in a class-action lawsuit.

Incident Response Support

- Federal-sponsored incident response support for organizations that are experiencing security incidents and need assistance getting through and recovering from the breach;
- Federal-sponsored cyber incident insurance modeled after FEMA to compensate for the retraction of private insurance carriers from the cyber insurance market;
- Expanded innovative law enforcement disruption of threat groups to reduce ecosystem risk creating the most harm to hospitals.

Regulatory Reform

- Revise HIPAA to reference the use of minimum standards in NIST CSF, HICP, or other recognized security practices, rather than prescribing cybersecurity requirements in statute. These standards should be built in partnership with the HSCC and regulators such as (OCR, ONC, CMS, and FDA) and cross-mapped for overlap or conflict across the various regulatory regimes intersect. A holistic, coherent cyber policy strategy is essential for a healthcare environment where clinical operations, medical devices, electronic health record technology, patient data, and IT systems are all interconnected but subject to different regulatory structures and authorities.

Conclusion

Mr. Chairman, 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 diagnose healthcare cybersecurity to be in a "stable condition."

Thank you.