Testimony of

Greg Garcia
Executive Director

of the

Healthcare and Public Health Sector Coordinating Council
Cybersecurity Working Group

on

"Securing the Future of Health Care: Enhancing Cybersecurity and Protecting Americans' Privacy"

Before the

United States Senate

Committee on Health, Education, Labor & Pensions

July 9, 2025

Summary of Recommendations

HSCC Cybersecurity Working Group

My statement today will offer what we believe the health sector and government need to do collaboratively to get ahead of ongoing cyber incidents and reduce their likelihood and impact.

First, the Administration should suspend any further consideration of the HIPAA Security Rule update published for public comment in January of this year and ***initiate a structured series of consultations and workshops with leaders in the health sector coordinated by HSCC to negotiate a modernized policy for healthcare cybersecurity resiliency, responsibility and accountability***.

Second, now well underway, is the need to ***perform a systemic health infrastructure mapping and risk assessment.*** This will provide industry and government visibility and risk management options involving critical services and utilities that support the many essential dependencies across the healthcare ecosystem and whose disruption could cause cascading disruption across the health system to the detriment of patient care, administrative operations and provider liquidity.

Third, reinstate the CIPAC framework by DHS to enable trusted collaboration with critical infrastructure industries and b) reauthorize the Cybersecurity Information Sharing Act of 2015, which enables trusted threat intelligence communications between industry and government but which sunsets this September.

Fourth, hold third party product and service providers and business associates to a higher standard of "secure by design and secure by default" for technology services and capabilities used in critical healthcare infrastructure.

Fifth, invest in a government-industry rapid response capability.

Sixth, invest in a cyber safety net for the nation's underserved providers, built on accountability and incentives.

Finally, over the next five years, the health sector and government have an all-hands on deck responsibility to ***implement the HSCC 5-year Health Industry Cybersecurity Strategic Plan.*** The plan recommends 10 end-state cybersecurity goals, and 12 implementing objectives to achieve those goals by 2029.
If we make progress against the goals and objectives, we can achieve an overall industry target state in which:

- Healthcare cybersecurity, both practiced and regulated, is made easier for practitioners and patients;
- Secure design and implementation of technology and services across the healthcare ecosystem is a shared and collaborative responsibility;
- Leaders in the healthcare C-suite own and invest in cybersecurity as an element of enterprise risk;
- A cyber safety net is in place to promote cyber equity across the ecosystem;
- Healthcare workforce is trained and capable in good cybersecurity as a wellness continuum; and,
- A "911 cyber civil defense" capability to lead early warning, incident response and recovery is reflexive and always on.

Cyber Safety is Patient Safety

Introduction

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

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

My testimony today will focus on four areas that will help inform both the diagnosis and prescription for healthcare cybersecurity:

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

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

***Third*,** how we should address health sector cybersecurity with a holistic approach.

The Health Sector Coordinating Council Cybersecurity Working Group

The HSCC CWG is a volunteer organization with a growing list of 470+ member organizations that operate under a charter-based governance structure with an elected Chair, Vice Chair and Executive Committee. Membership is open to organizations that are a) covered entities or business associates under HIPAA; b) health plans or payers; c) regulated by FDA as a medical device or pharmaceutical company; d) health IT companies subject to health data interoperability rules; e) public health organizations and f) any healthcare industry associations or professional societies. A small allotment of "Advisor" members – consulting, law, and security companies - is permitted to participate and support CWG initiatives pro bono.

While the CWG is focused on cybersecurity best practices, policy and long-term strategy, our key operational partner in critical infrastructure protection – the "firefighter" - is the Health

Information Sharing and Analysis Center, which is the nation's primary information sharing and incident response organization for the heath sector.

The HSCC CWG is currently organized into numerous function-specific, outcome-oriented task groups composed of 50 to 190 organizations across the health industry and government that develop sound cybersecurity practices and resources for various healthcare cybersecurity disciplines. These disciplines include health provider cybersecurity management; artificial intelligence cybersecurity; incident response and operational continuity; third party and systemic risk, medical technology security, and many others.

With those cross-functional cybersecurity collaborative efforts, since 2019 the CWG has published 26 sound practices and guidance documents and 15 policy advisories that address our 2024-29 Health Industry Cybersecurity Strategic Plan, which is discussed beginning on page 19 of this statement. These resources, developed by the sector for the sector, are freely available on our website at https://healthsectorcouncil.org/hscc-publications/. Several of these publications are under joint seal by HSCC and HHS as a demonstration of our shared resolve and vision for essential cybersecurity programs that all health organizations should implement.

One of these – the *Health Industry Cybersecurity Practices (HICP)* - is recognized under P.L. 116-321, signed by President Trump on January 5, 2021, as a set of controls which, if

implemented by an entity prior to a breach that becomes subject to HIPAA enforcement action, would be a mitigating factor in the consideration of punitive fines and audits by HHS.

Foundationally, the HSCC Cybersecurity Working Group (CWG) serves as an advisory council to the sector, HHS, CISA, and other government agencies with a critical infrastructure protection mission. This construct involving all public-private partnerships between government and 17 designated critical infrastructure industry sector coordinating councils is promulgated in national policy going back to 1998, most recently updated in President Biden's National Security Memorandum 22 in 2024 and President Trump's Executive Order 14028 in 2021. It is a working partnership in which critical sectors and their associated government agencies collaborate to identify and mitigate systemic physical and cyber threats to the security and resiliency of critical healthcare infrastructure, develop guidance and policies for mitigating those risks, and facilitate threat preparedness and incident response.

This framework has been functioning for 20 years on the authorities of the Critical Infrastructure Partnership Advisory Council (CIPAC) framework administered by the Department of Homeland Security. CIPAC allows government agencies to pursue ongoing engagement and planning with industry sector coordinating councils against systemic cyber and physical security threats, exempt from normal federal advisory committee public disclosure rules that would otherwise compromise sensitive threat, vulnerability and mitigation information.

The CIPAC framework, however, was cancelled in January of this year and consequently our government partners have been required to suspend substantive engagement with industry on critical infrastructure planning and strategy, potentially jeopardizing our collaborative risk identification and mitigation and the nation's critical infrastructure security and resiliency. There is little disagreement across our nation's essential industries that this partnership has been fruitful and evolving and should be reinstated.

A Health System Under Constant Attack

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

Threat actors are motivated to leverage ransomware attacks to monetize stolen health data, and operational disruptions. The cybersecurity focus in healthcare has traditionally been on privacy and protection of healthcare data, but when healthcare data is manipulated or destroyed, and health delivery organizations (HDOs), their suppliers, service providers and payment systems are rendered inoperable, as seen in recent ransomware incidents, patient lives can be at risk. This threat is particularly acute for small, rural, critical access and

underserved, under-resourced health providers that are operating on razor thin or negative margins and haven't the capability to make sufficient investments in cyber preparedness and response programs.

Ransomware and other disruptive cyber attacks

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

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

- Medical devices stop working, or their settings are corrupted, risking danger to the patient.

Business Risks

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

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

Why this is Happening

The reasons that the health sector falls prey to these types of attacks stem from the increasing complexity of today's connected healthcare ecosystem, which presents potentially massive systemic cyber risks:

- unanticipated and poorly understood interdependencies;
- unknown inherited security weaknesses;
- vendor solutions that do not adhere to cybersecurity standards;

- systems that fail to account adequately for human factors related to cybersecurity controls; and
- inconsistencies between software and equipment lifecycles, among others.

In addition, we are adopting new technologies faster than we are updating security practices, therefore creating a growing gap between slowly developing security preparedness and rapidly evolving security threats.

The business and delivery of healthcare are evolving through the adoption of digital consumer wellness and fitness technologies, remote care models, and accelerating consolidation of health systems, third-party vendors, and new disruptive healthcare business models. As a result of these drivers, healthcare frequently occurs outside of hospitals and clinician offices, which requires transmission of telehealth, remote care, and home health data across uncontrolled home and public networks and cloud services. Further, valuable data derived from personal lifestyle devices such as fitness trackers and smart watches can now augment clinical data and decisions.

Cybersecurity controls for these technologies are often beyond the oversight of the traditional healthcare regulatory and oversight mechanisms. The result is technologies that are becoming increasingly important in the healthcare ecosystem but lacking common cybersecurity protections.

Recommendations for Holistic Healthcare Cybersecurity

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

This imperative can be addressed through negotiated cybersecurity regulation, policy, and voluntary practices implemented across the healthcare ecosystem. It is clear that, given the increasing number and types of cyber incidents impacting the healthcare ecosystem, neither voluntary practices nor government policy have been sufficient to reduce cyber risk and incidents across the sector.

Accordingly, the HSCC offers considerations for how government policy and programs can support the health sector's investment in and management of stronger cybersecurity risk reduction. These proposals are neither exhaustive nor rigid in their descriptions. Rather, by focusing more on the "what" – objectives and outcomes - than on the "how" – specific requirements and processes, these recommendations are meant to stimulate creative discussion between government and industry about initiatives that can measurably improve cybersecurity management across the health sector.

1. Our most immediate policy recommendation, as submitted to the Administration in April, is that the ***Administration suspend any further consideration of the HIPAA Security Rule update published for public comment in January of this year and initiate a structured series of consultations and workshops with leaders in the health sector coordinated by HSCC to forge consensus on a modernized policy for healthcare cybersecurity resiliency, responsibility and accountability***. Such an approach would operationalize Trump Administration executive orders on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure in 2017 and Achieving Efficiency Through State and Local Preparedness released in March 2025.

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

flexible to meet ever-evolving threats and disruptive technology, cost-efficient, and effective at measurably improving cybersecurity outcomes.

An appropriate starting point for these negotiations would be the HHS-HSCC "Health Industry Cybersecurity Practices" and the Cybersecurity Performance Goals that the industry and HHS jointly developed following data analyses of how the industry is most frequently and severely disrupted by cyber attacks. Enveloping these frameworks over a longer term strategy is the 2024-25 Health Industry Cybersecurity Strategic Plan, published by HSCC in February 2024 with participation from officials in HHS and CISA. If widely implemented across our ecosystem using a combination of mandatory and flexible objectives, these resources and the 25 others negotiated among health industry stakeholders since 2019 would constitute robust cybersecurity programs that we can agree to be held accountable to and would measurably move the needle against our evolving cyber threats.

2. A priority operational recommendation for this year, which is now underway and soon to be released, is to support and ***operationalize national health infrastructure mapping and risk assessment to provide visibility and risk management options involving critical services and utilities that support the many interconnected interdependencies across the healthcare ecosystem and may be subject to chokepoint vulnerabilities***.

We are acutely aware that all of our core health delivery, financial and operational work flows - whether claims processing, lab and blood management, medical imaging, and other healthcare services – depend on IT, software and digital services that, if severely disrupted or disabled by cyber attack, would cause cascading and crippling impact on our national economic security and public health and safety. These utilities such as software programs, processing applications and specialty communications platforms are often unknown and taken for granted, but without which the very delivery and financing of healthcare would not be accomplished.

There is in fact a policy framework in place – Section 9 of Executive Order 13636 of 2013 - which directs DHS and sector agencies to identify those "critical infrastructure entities where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

This responsibility requires industry leaders from across the healthcare subsectors – health providers and health IT, insurers and plans, pharmaceutical and medical technology companies, and public health agencies -- to identify those critical functions and assets, their connect points and dependencies, the associated concentration risk from mergers and acquisitions, and the relative risk to the provision of healthcare – both immediate impact and duration - that those functions would pose if disrupted. It is about understanding concentration risk, levels of redundancy of similar services, and the adequacy of both physical and cyber protective measures to support the security and resiliency of those critical utilities.

This process will take time to get it right, even as it will never be fully accurate given the constantly shifting architecture of our complex healthcare system.

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

3. In order for some of our industry initiatives to have maximum benefit to the sector, the government needs to engage actively in this public-private partnership to help guide policy and risk management approaches by industry. That means: a) ***reinstatement of the CIPAC*** framework by DHS to enable trusted collaboration and b) Congressional ***reauthorization of the Cybersecurity Information Sharing Act of 2015*** which enables trusted threat intelligence communications between industry and government but which sunsets this September. Many industry across the critical infrastructure spectrum have urged the Congress to act on this impending expiration, and we echo that.

4. Related to critical function assessment is the imperative to ***hold third party product and service providers and business associates to a higher standard of "secure by design and secure by default" for technology services and capabilities used in critical healthcare infrastructure***. More than half of all data breaches on health systems are through business associates; many ransomware attacks similarly find their way into enterprise networks through third parties. Many medical devices continue to be delivered to the customer with security vulnerabilities, with uneven attention to the security imperative among device manufacturers. This also includes the growing number of non-traditional healthcare technology providers – like cloud service providers, wearables and data analytics/AI solutions – that are playing an increasingly more important role in the healthcare ecosystem and with access to highly sensitive personal information.

What this means is that:

- HIPAA Covered Entities and Business Associates should be held more accountable and required to demonstrate compliance with improved minimum baseline security requirements, which tracks back to recommendation #1 above. Existing minimum HIPAA security rule requirements are too low, but the proposed HIPAA security rule updates introduce significant administrative burden without focus on cybersecurity baseline improvements that will successfully counter ransomware and other cybersecurity risks. Increased accountability should be addressed through recommendation #1 (collaboration for updating HIPAA security rule requirements

and other health sector cybersecurity needs to ensure effective minimum requirements).

- FDA progress should be monitored for the implementation of their new "524B" authorities to verify intended improved outcomes in medical device cybersecurity posture.
- For unregulated healthcare technology and service providers with no access to health data or essential clinical and administrative workflow functions, incentives such as reduced compliance risk should be identified and enacted to encourage demonstrated implication of minimum baseline security requirements.

5. ***Invest in a government-industry rapid response capability***. Emergency response, recovery and business continuity remain ongoing challenges for private sector and government stakeholders alike. The Change Healthcare attack in February 2024 exposed significant challenges for health systems to maintain business resiliency and continuity and for government and payers to provide time sensitive operational and financial backup for providers in dire straits. Much of our health system and patient care depend on minutes, hours and days, not on months. We need to invest in a rapid response force, or as we call it a "Healthcare 911 Cyber Civil Defense" against systemic attacks. This rapid response force can use government authority to declare "national cyber emergency", activate catastrophic national cyber insurance to supplement private insurance, provide fast financial support, permit temporary suspension of certain regulatory chokepoints and provide mobile healthcare

capability to assist those in dire need. Success in this effort would demonstrate a next-generation end-state we call for in our Health Industry Cybersecurity Strategic Plan, discussed below. This need is particularly important for the "target rich, cyber poor" small, rural, critical access, Federally Qualified Health Centers and other resource-constrained health providers across the nation.

6. **Invest in a cyber safety net for the nation's resource-constrained providers**, built on accountability and incentives. As discussed, the nation's resourced-constrained health systems are the most vulnerable to cyber threats, lacking the resources and expertise to invest in basic cyber hygiene requirements. In May of this year the HSCC Cybersecurity Working Group released "On the Edge: Cybersecurity Health of the Nation's Resource-Constrained Health Providers" – a white paper of findings and recommendations resulting from interviews with 40 health providers in 30 states about their cybersecurity challenges and needs from government and the community to meet their cybersecurity obligations to patient safety. While the HSCC has produced so many practical tools to close the gap between cyber threats and preparedness among the nation's resource-constrained providers, the issue of awareness and resources remain as impediments to adoption and implementation. Many of the smaller, underserved providers in our membership have expressed the same observation that they will invest in strengthened cyber defenses if they are told to do so, but that if given the choice between hiring a nurse to care for patients or hiring a cybersecurity professional, the Hippocratic Oath of "first do no harm" must prevail. But under the principle that "cyber safety is patient safety"

many providers would acquiesce to minimum mandatory cyber controls as long as they are financially or operationally supported.

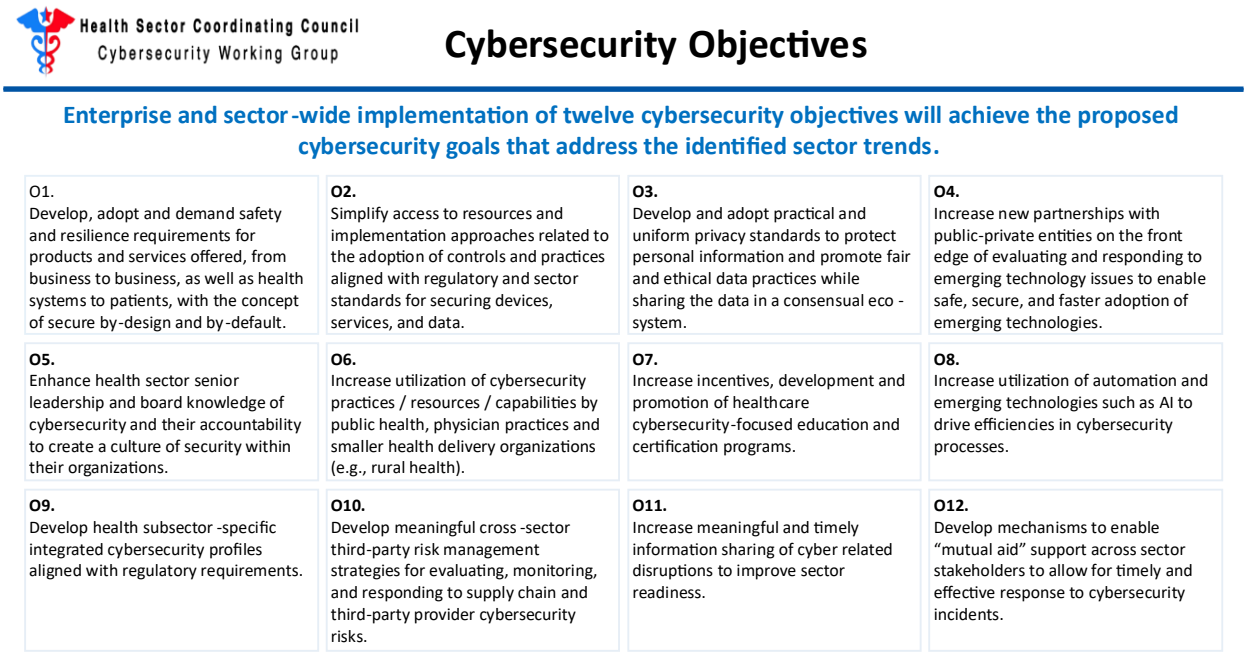
7. Finally, over the next five years, the industry and government have an all-hands on deck responsibility to contribute to ***achievement of the 5-Year Health Industry Cybersecurity Strategic Plan*** - https://healthsectorcouncil.org/cyber-strategic-plan/ published by the HSCC Cybersecurity Working Group in February of last year.

The Strategic Plan projects 7 major industry trends in the health sector over the next 5 years and presents a sector-wide call to action for healthcare organizations to address those trends and increase their individual and collective cyber resilience for an interconnected industry. The intent of this document is to guide C-suite executives, information technology and security leaders, government and other relevant stakeholders toward investment and implementation of strategic cybersecurity principles which, if adopted, will measurably reduce risks to patient safety, data privacy, and care operations which can cause significant financial, legal, regulatory, and reputational impact.

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

The plan presents 12 implementing objectives (see Figure 1 below) that the industry as a whole including the government must address collaboratively to achieve a higher, more persistent and reflexive state of healthcare cybersecurity by 2029.

Figure 1



Conclusion

Mr. Chairman and Members of the Committee, we have a tremendous amount of work to do in the health sector to make the policy and programmatic investments necessary to upgrade our cybersecurity diagnosis from critical to stable condition. We have been working hard on the prescription – some of it will be bitter medicine, some of it should be simple and

habitual. We also know we will never be totally immune from evolving cyber infections; we will only be better. That is the nature of this threat.

If we succeed, however, we can look to a healthcare system over the next five years that will have evolved with measures of progress toward better sector-wide cyber wellness:

- Healthcare cybersecurity – both practiced and regulated – is reflexive, evolving, accessible, documented and implemented for practitioners and patients.
- Secure design and implementation of technology and services across the healthcare ecosystem is a shared and collaborative responsibility.
- The healthcare C-Suite embraces accountability for cybersecurity as enterprise risk.
- A Cyber Safety Net of financial, policy and technical assistance supports cyber equity across the ecosystem.
- Workforce cybersecurity learning and application is an infrastructure wellness continuum.
- A "911 Cyber Civil Defense" capability ensures that early warning, incident response and recovery are reflexive, collaborative, and always on.

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. And through continued and expanded engagement in our collective purpose, broader awareness promotion, and forward-

leaning government programs and support, we can move the needle and five years from now upgrade the healthcare cybersecurity diagnosis from “critical” to “stable condition.”

This concludes my testimony, thank you.

##

Submitted for the record:

- Health Industry Cybersecurity Strategic Plan - https://healthsectorcouncil.org/the-plan/
- HSCC Proposal for Healthcare Cybersecurity Consultations: https://healthsectorcouncil.org/government-partners-forward-path-2025-cyber-policy-statement
- HSCC cybersecurity policy, programmatic and regulatory recommendations for government consideration - https://healthsectorcouncil.org/health-industry-cybersecurity-recommendations-for-government-policy-and-programs/

The Appendix that follows is a compendium of detailed recommendations and ideas for evolved policy and operational approaches to healthcare to healthcare cybersecurity, adapted from our March 2025 recommendations.

Appendix

Health Sector Coordinating Council Cybersecurity Policy and Program Proposals for Government Consideration

To organize our prescriptions for cyber health in the health sector, the HSCC coalesces around our 2024-29 *Health Industry Cybersecurity Strategic Plan (HICSP)*. The Strategic Plan in turn can be organized into broad *Themes for Cyber Wellness* that guide our activities toward end state goals.

Together, these guiding foundations help categorize interrelated approaches to our cybersecurity challenges. They establish the principles by which we propose and negotiate policy, investment, and assistance programs. And they present a framework for identifying and holding accountable our shared responsibilities for voluntary cybersecurity management that evolves with the threat, and mandatory requirements that set uniform baselines for regulatory compliance.

The *Cyber Wellness Themes* are: ***Access*** - the notion that resources and understanding about managing our cyber environment should be accessible, simple, and implementable with a culture of security; ***Community*** – imagining a "911 Cyber Civil Defense" of mutual aid, collaborative preparedness and incident response on the principle that the adversary must beat all of us to beat one of us; ***Innovation*** – that we continue to develop and adopt new technologies in healthcare and security, while we innovate how we manage our healthcare cybersecurity environment, constantly learning, adapting, and evolving to meet the ever-changing threat landscape; and ***Workforce*** – filling the workforce gap in cybersecurity for healthcare by building a pipeline of next generation cyber leaders while innovating in workforce training about the fundamentals of cyber hygiene.

The following policy and programmatic recommendations are offered for HHS, CISA, Congress and other Federal agencies to support healthcare cybersecurity. The recommendations are grouped into the following topical categories, linked here to their location in the document: 1) Preparedness and Information Sharing; 2) Financial Support and Incentives; 3) Incident Response and Recovery; 4)

Workforce; and 5) Regulatory Reform, and align with the HSCC's "Cyber Wellness" themes of ***Access, Community, Innovation*** *and* ***Workforce*** and many of the twelve implementing Objectives captained in the sector's five-year Cybersecurity Strategic Plan.

1. Preparedness and Information Sharing

The following Preparedness and Information Sharing recommendations operationalize the HSCC cyber wellness themes of ***Access, Community*** *and* ***Innovation,*** *and address numerous Health Industry Cybersecurity Strategic Plan Objectives.*

1.1 HHS should join with the HSCC and healthcare stakeholders in a national communications and outreach campaign to the health provider community and its supporting infrastructure about the imperative of cyber security as a patient safety issue. This begins with a federated communications strategy featuring the many healthcare-specific cybersecurity practices offered by industry and government that help users to 1) monitor threats; 2) manage risks; 3) secure medtech; 4) respond and recover; and 5) measure effectiveness.

1.2 Joint security guidance published by HHS and HSCC tend to have more credibility, reach and adoption than publications released independently by either. Procedures for developing joint publications should be formalized and structured similar to how the HHS 405(d) program and HSCC produced the flagship cybersecurity guide "Health Industry Cybersecurity Practices (HICP)– Managing Threats and Protecting Patients" and the "Hospital Resiliency Cyber Landscape Analysis".

1.3 Strengthen the 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.

1.4 Remove potential regulatory or legal barriers (eg., antitrust, Stark law, etc) to the formation of a health provider consortium that would develop and promote uniform minimum cybersecurity program requirements for any entity that sells hardware, software or services to a health system. This could be modeled on, for example, a FEDRAMP-type govt conduit to 3rd party cyber risk management

requirements using a version of the HSCC Model Contract - https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2.

1.5 Generally 50% of healthcare breaches and ransomware attacks on healthcare are due to breaches against third party technology and service providers; we should accordingly explore national-security based regulatory mechanisms to hold technology, software and service providers supporting critical health infrastructure to higher levels of accountability for enhanced product and enterprise cybersecurity requirements, similar to FDA pre-market and post-market cybersecurity requirements on medical device manufacturers subject to safety and quality standards, using a cleared entities list approach similar to FEDRAMP.

1.6 Designate high impact cyber and ransomware attacks, which result in widespread disruption and delay of health care delivery at critical access, safety net and rural emergency hospitals, as “all hazards” incidents to activate appropriate Federal government response support for state, regional and local emergency response services.

1.7 HHS should encourage health sector organizations to join and actively participate in the Health-Information Sharing and Analysis Center (Health-ISAC) or other information sharing and analysis organizations as part of a robust resilience strategy. The U.S. Department of Treasury set the precedent in 2014 in issuing a statement recommending that all financial institutions "... participate in the [Financial Services] ISAC as part of their process to identify, respond to, and mitigate cybersecurity threats and vulnerabilities....Rapidly evolving cybersecurity risks reinforce the need for all to have methods for obtaining, monitoring, sharing, and responding to threat and vulnerability information (*source*)." HHS should adopt a similar recommendation with appropriate financial support and incentives particularly for resource-constrained health providers described below so that healthcare and public health organizations can benefit from the rapid sharing of cybersecurity risks and mitigating controls.

1.8 Cyber insurance carriers have varying and inconsistent cybersecurity control requirements for determining premiums and coverage of insured healthcare entities. For cyber risk reduction and risk transfer efficiencies to scale across the sector, consistency in expectations is needed for assessing

providers' investments in risk management programs. Accordingly, HHS and CISA should coordinate with major cyber insurance carriers and their state regulatory agencies to encourage the reference of HICP into cyber insurance policy requirements, similar to the incentive signed into law as P.L. 116-321 on January 5, 2021. This law recognized breached entities' implementation of HICP, the NIST Cybersecurity Framework and other recognized security practices as mitigating factors that HHS must consider when pursuing a HIPAA data breach enforcement action. Reference practices could also include participation in the Health-ISAC or other information sharing and analysis organizations (ISAO's) as an element of good cybersecurity practice that would improve premiums and coverage.

1.9 Protect health delivery organizations from class action lawsuits if they can demonstrate that they implement NIST CSF, HICP, or other recognized cybersecurity practices. This could incentivize more robust adoption and implementation of security controls.

1.10 Continue development, outreach and provision of innovative CISA support programs, such as the Cyber Hygiene (CyHy) program and cyber exercises, that can be tailored in close consultation with HHS to healthcare entities.

1.11 Government sharing of cyber threat and incident intelligence frequently does not meet private sector needs because it is not timely, relevant or actionable. When developing threat and remediation advisories for the health sector, CISA, HHS and law enforcement should, as a matter of protocol under MOU, consult with designated industry sector leaders through Health-ISAC and HSCC with credible – and as appropriate, global - threat intelligence and analysis that can be compared and reconciled with government intelligence ahead of an advisory release. This would ensure that both industry and government leaders are generally aligned – rather than sending inconsistent messages - before publication to the broader community about the accuracy of the intelligence, its relevance to and impact on the sector, and appropriate remediation procedures.

1.12 Tailor a classified information sharing program involving health sector-designated liaison representatives, CISA, HC3, and law enforcement agencies, so that the liaison representatives can provide consideration and feedback to federal threat analysts on what is most relevant and actionable to the Sector.

1.13 Consider incentives, support and protections for health systems working with government in various forms of proactive operational collaboration against threats and attacks, impending or in-process. This may require reauthorization of the protections contained in the Cybersecurity Information Sharing Act of 2015 (CISA), sunsetting in 2025, which aims to improve cybersecurity by encouraging information sharing between private sector entities and government agencies about cyber threats, allowing them to collaborate more effectively in identifying and mitigating cyberattacks, while also providing legal protections for companies sharing this information.

2 Financial Support and Incentives

*The following Financial Support and Incentives recommendations operationalize the HSCC cyber wellness themes of **Access** and **Community,** and address numerous Health Industry Cybersecurity Strategic Plan Objectives.*

2.1 CMS reimbursement incentives: If an institution demonstrates implementation of HICP, the NIST CSF, or other recognized security practices as incentivized in P.L. 116-321 as mitigation for HIPAA-enforcement liability following a data breach, CMS similarly can offer additional reimbursement under a concept of "meaningful protection." This could include additional CMS reimbursement to HDO's participating in the Health-ISAC or other ISAO's, implementation of active legacy medical technology cyber security management and replacement programs, and cybersecurity being included among performance goals overseen by hospital boards. Such incentive programs could be phased-in, measuring progress over time, aligning with HICP or other recognized security practices and tying incentives to the cost/difficulty/scale of particular control frameworks and other cybersecurity investments in the clinical environment.

2.2 Unregulated third-party technology and service providers represent both a major threat vector and costly third-party risk management demands. Health providers should not bear sole burden for policing their vendors; such third parties must be held to an enforceable higher cybersecurity standard when they support critical healthcare infrastructure where lives are at risk.

2.3 Workforce augmentation for needed cybersecurity skills should be funded at the federal level through ongoing commitment of CISA technical support programs, and at the federal and state levels for subsidizing the use of contracted managed security providers, academic institutions' deployment of student engineers and cybersecurity majors in programs such as the Consortium of Cybersecurity Clinics (https://cybersecurityclinics.org/); state national guard assistance for cybersecurity incident response, and other programs.

2.4 Maintain and expand of the U.S. Department of Agriculture's Rural Loan Program, which supports rural entities such health providers with various forms of cybersecurity support:

- Funding equipment and infrastructure
- Securing rural development's portfolio through managing risk to healthcare facilities
- Potential technical assistance provider
- Conduit to rural community leaders and health care providers to share information and resources
- As one-time grant support payments generally cannot be used for hiring, grant programs should be tailored to the specific needs the Resource-Constrained health providers and should be ongoing as part of the payment structure.

2.5 CISA and HHS should encourage state insurance regulatory agencies to work with insurance companies to devise incentive programs that tie reduced premiums and/or improved coverage for cyber insurance to participation in the Health-ISAC and other information sharing and analysis organizations as one element of an appropriate cybersecurity risk management program.

2.6 HHS should explore mechanisms to fund or incentivize qualified managed security service providers (MSSPs) to assist critical access, safety net and rural emergency hospitals to remediate urgent vulnerabilities or mitigate threats. Many organizations struggle to take advantage of information made available via various channels including agencies, information sharing organizations, product vendors, etc. State, regional, local support services can partner with FBI and CISA offerings to enhance health sector security.

2.7 HHS should establish needs-based subsidy and incentive programs to help resource-constrained health systems wanting to improve situational awareness by participating in the Health-ISAC or other information and sharing and analysis organizations.

2.8 Add specified cybersecurity tools; services and surge workforce capacity as allowable expenses under the FCC Health Connect Fund subsidy of the Universal Service Administrative Company (USAC). This would leverage the purchasing power of under-resourced systems to supplement the current and more narrow WAN/Core Network investment expense.

2.9 HHS should compile a reference of federal subsidies and grants across the government that fund cybersecurity services, tools, and education for health providers.

3. Incident Response and Recovery

*The following Incident Response and Recovery recommendations operationalize the HSCC cyber wellness themes of **Community** and **Innovation**, and address numerous Health Industry Cybersecurity Strategic Plan Objectives.*

3.1 [repeated from above] Government sharing of cyber threat and incident intelligence frequently does not meet private sector needs because it is not timely, relevant or actionable. When developing threat and remediation advisories for the health sector, CISA, HHS and law enforcement should, as a matter of protocol under MOU, consult with designated industry sector leaders through Health-ISAC and HSCC with credible – and as appropriate, global - threat intelligence and analysis that can be compared and reconciled with government intelligence ahead of an advisory release. This would ensure that both industry and government leaders are generally aligned – rather than sending inconsistent messages - before publication to the broader community about the accuracy of the intelligence, its relevance to and impact on the sector, and appropriate remediation procedures.

3.2 Government information and incident response interfaces with industry should clearly articulate and rapidly-deliver actionable intelligence when implementing its cyber incident reporting collection and analysis authorities.

3.3 Because health systems are burdened with multiple differing report forms and overlapping agency requirements for the same incident, incident reporting timeframes and methodologies should be standardized across government regulatory entities.

3.4 Cyber-attack victim reporting requirements should be waived while an incident response is underway in the early stages of discovery and operational triage.

3.5 Provide federal-sponsored incident response support for organizations that are experiencing security incidents and in need of assistance getting through and recovering from the breach. Expand innovative law enforcement disruption initiatives against both foreign and domestic threat groups to reduce ecosystem risk creating the most harm to hospitals.

3.6 As incentives for voluntary reporting and information sharing with the government, the same civil, regulatory, FOIA and anti-trust protections provided under CISA 2015 for cyber threat information sharing with the federal government should be provided for: 1) victim organizations that have implemented recognized cybersecurity practices, as defined under PL 116-321 and 2) discussions with government to determine impact of attack on public health and safety.

3.7 Provide Military, State, or National Guard cyber/medical personnel, equipment and services support for providers meeting specific need thresholds after an attack (incident response and recovery), with appropriate reimbursement from HHS/CISA.

3.8 Partner government and industry research support toward technical and operational efficiencies for effective incident response and continuity to ensure rapid return to health delivery operations following a severe cyber attack.

4. Workforce

*The following Workforce recommendations operationalize the HSCC cyber wellness themes of **Access** and **Workforce**, and address numerous Health Industry Cybersecurity Strategic Plan Objectives. A number of recommendations supplement those made in the May HSCC report – "On the Edge – Cybersecurity Health of America's Resource-Constrained Health Providers."*

4.1 HHS should administer a healthcare cybersecurity workforce development and cyber training program with assistance from NIST, CISA, and/or Veterans Administration. A program could include access to free cyber training, assistance to providers under an expanded Regional Extension Centers program, and student loan forgiveness programs modeled after physician loan forgiveness programs, or the National Science Foundation's CyberCorps® 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.

4.2 Fund federal, and supplement state-subsidized - "civilian cyber health corps" programs. This could take the form of loan forgiveness; i.e., a Federal program pays / helps pay for a cyber education in exchange for a minimum number of years served, modeled after a uniformed health corps such as the U.S. Public Health Service Commissioned Corps - https://www.hhs.gov/surgeongeneral/corps/index.html. Also suggest establishing career pathways that do not require a full 4 years of college (i.e. certificate programs and associates).

4.3 Augment workforce development programs such as in the HITECH Act, which funded health IT workforce training programs: the University-Based Training Program and Community College Consortia Program. In total the two programs trained 21,437 students from all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands at 91 academic institutions. See: https://www.healthit.gov/data/quickstats/hitech-workforce-development-programs.

4.4 HHS should explore mechanisms to fund or incentivize qualified managed security service providers (MSSPs) as workforce augmentation to assist critical access, safety net and rural emergency hospitals to remediate urgent vulnerabilities or mitigate threats. Many organizations struggle to operationalize information provided by government agencies, information sharing organizations, product vendors, etc. State, regional, local support services can partner with FBI and CISA offerings to enhance health sector security.

4.5 HHS should establish needs-based subsidy and incentive programs to help resource-constrained health systems wanting to improve situational awareness by participating in the Health-ISAC or other information and sharing and analysis organizations (ISAOs).

4.6 Add specified cybersecurity tools, services and surge workforce capacity as allowable expenses under the FCC Health Connect Fund subsidy of the Universal Service Administrative Company (USAC). This would leverage the purchasing power of under-resourced systems to supplement the current and more narrow WAN/Core Network investment expense.

4.7 HHS should compile a reference of federal subsidies and grants across the government that fund cybersecurity services, tools, and education for health providers.

4.8 Map the NICE Framework's Work Roles and Job Descriptions to HICP to bring better and clarity and uniformity to matching skills with job descriptions - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

5. Regulatory Reform

The following Regulatory Reform recommendations operationalize the HSCC cyber wellness theme of ***Access,*** *and address numerous Health Industry Cybersecurity Strategic Plan Objectives.*

5.1 As the primary cross-sector healthcare advisory council focused exclusively on critical infrastructure cybersecurity, the HSCC is prepared to engage with government leadership in a phased series of policy consultations and workshops to negotiate a modernized, coherent, practical, scalable and effective framework that combines both mandatory and flexible voluntary practices for healthcare technology, enterprise and health provider cybersecurity. A successful model for this type of public-private engagement is the development of the NIST Cybersecurity Framework initially published in 2014 after 1 year of work, a process convened and guided by NIST with content generated by the industry owners and operators of critical infrastructure – those most knowledgeable and responsible for securing it.

The December 2024 HHS notice of proposed rulemaking updating the HIPAA Security Rule did not demonstrate sufficient insight to the complexities of achieving effective cybersecurity protections

for the health sector, nor acknowledge the considerable work the sector and government partners have accomplished in good faith and urgency over the past 6 years to build a collective cyber defense. The HIPAA Security Rule update process should be reset with the collaborative process described above.

5.2 As recommended in the 2017 Health Care Industry Cybersecurity Task Force report, HHS should work across the regulatory Operating Divisions (ASPR, OCR, ONC, CMS, FDA) and other cyber- and data-regulating government entities involving cybersecurity and privacy (FTC, SEC, etc) to cross-map and harmonize regulatory requirements on health systems that duplicate or conflict. A holistic, coherent cybersecurity 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 differing regulatory structures and authorities.

5.3 Enhance CMS fraud protection programs to reduce the value and thus demand of stolen ePHI and other data, and thus attempts at cyber exploitation.

5.4 Harmonize current sector specific regulations to possible future regulations on Consumer Data Privacy and Security as well as Artificial Intelligence to further create a holistic, coherent strategy with clearly-aligned requirements and regulatory authority.

##