Testimony of

Greg Garcia
Executive Director for Cybersecurity

of the

Healthcare and Public Health Sector Coordinating Council
Cybersecurity Working Group

on

"*Examining Legislative Proposals to Reform Medicare Provider Payment and Bolster Health Care Cybersecurity*."

Before the

United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Health

September 15, 2026

Summary of Testimony

- The cybersecurity legislation pending before the committee – the *Healthcare Cybersecurity and Resiliency Act of 2026* and the *Rural Hospital Cybersecurity Enhancement Act* – are a welcome indication of the Committee's attention to this complex and evolving challenge. These bills read as complementary guidance for: 1) structured coordination processes and objectives across the U.S. Department of Health and Human Services (HHS), the Cybersecurity and Infrastructure Security Agency (CISA), and the healthcare industry sector, and 2) specific, targeted assistance to the nation's small, rural, and resource-constrained health providers. Where clarifications or refinements are needed in certain provisions, the HSCC stands ready to work with the committee and offer our recommendations.

- The Health Sector Coordinating Council Cybersecurity Working Group is an industry advisory council working with the government – particularly the U.S. Department of Health and Human Services – in a national critical infrastructure public-private partnership conceived under a series of presidential executive orders. The Council is focused on developing best practices, guidance and programmatic initiatives for use by the sector, coupled with advising the government about optimal policy and programmatic support for the systemic security and resilience of the nation's critical healthcare infrastructure and patient safety.

  Our nearly 40 actionable guidance resources are prepared to substantially improve the cybersecurity risk management programs by the nation's small, medium and large critical healthcare entities and to do so with a view of their cross-sector, systemic interdependencies that make this mission a shared challenge and a shared responsibility. As such, the government's support and amplification of the partnership and our counsel will demonstrably improve the uptake and implementation of these resources that will measurably improve the security and resiliency of the sector. This applies to cybersecurity preparedness and incident response, workforce development, regulatory simplification, support for rural and resource-constrained health providers, and greater cybersecurity discipline for unregulated third-party technology and service providers that support the business, operations and delivery of health care.

- The nation's rural and resource-constrained health providers remain the most vulnerable and unprepared to protect against evolving cyber threats and technological innovation – both beneficial and adversarial. This calls for a concerted, multi-pronged combination of government programs, assistance, and funding with market-based mutual support and community defense.

##

Introduction

Chairman Guthrie, Ranking Member Pallone, Subcommittee Chairman Griffith, Ranking Member DeGette, and members of the Committee, I am Greg Garcia, Executive Director of the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG). The CWG is an industry-led advisory council of almost 500 healthcare organizations and government offices working together 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 40 years of executive management in cybersecurity and related national and homeland security concerns. I have navigated and advised on the intersecting languages of policy, technology, 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 coordination 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;

Third, a review of the two cybersecurity bills under consideration by the committee – the *Healthcare Cybersecurity and Resiliency Act of 2026* and the *Rural Hospital Cybersecurity Enhancement Act;* and

Fourth, a sampling of HSCC cybersecurity resources and initiatives along with our recommendations to government and their alignment with pending committee legislation.

Health Sector Coordinating Council Cybersecurity Working Group

The HSCC Cybersecurity Working Group (CWG) is a volunteer advisory council of almost 500 member organizations operating under a charter-based governance structure with an elected Chair, Vice Chair and Executive Committee. Membership is open to regulated healthcare organizations that are a) covered entities or business associates under HIPAA; b) health plans or payers; c) regulated by FDA as medical device or pharmaceutical companies; d) health IT companies subject to health data interoperability rules; e) public health organizations and f) any healthcare industry associations or professional societies representing the above. 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 (Health-ISAC), which is the nation's primary information sharing and incident response organization for the health sector.

Foundationally, the HSCC Cybersecurity Working Group serves as an advisory council to the sector, HHS, CISA, and other government agencies with a critical infrastructure protection mission. This construct involving public-private partnership between government and 17 designated critical infrastructure industry sector coordinating councils is promulgated in national policy going back to 1998, most recently updated in National Security Memorandum 22 in 2024 and Executive Order 14028 in 2021. It is a working partnership in which critical sectors and their associated government agencies collaborate to share information, identify and mitigate systemic physical and cyber threats to the security and resiliency of critical infrastructure, develop guidance and policies for mitigating those risks, and facilitate threat preparedness and incident response. The formal chartering and oversight of this partnership have historically been overseen by the Cybersecurity and Infrastructure Security Agency (CISA) since 2004 and is currently being updated as a program known as the Alliance of National Councils for Homeland Operational Resilience – Critical Infrastructure, or "ANCHOR-CI."

The HSCC CWG is 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 priority 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, the CWG has published 38 practices and guidance documents since 2019 (and several on the way before the end of 2026) and 15 policy advisories that address our 2024-29 Health Industry Cybersecurity Strategic Plan. 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, for example, is the *Health Industry Cybersecurity Practices (HICP)* which is recognized under P.L. 116-321 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 HHS consideration of punitive fines and audits. This is one example of the value of this public private partnership framework, in which joint efforts such as HICP enjoy the credibility and adoption of the nation's healthcare institutions and Congressional authority.

Why We Are Here: A Health System Under Constant Attack

The reference to "healthcare cybersecurity" was infrequently 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 use ransomware attacks to monetize stolen health data, and operational disruptions. The cybersecurity concerns related to healthcare have traditionally been about 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 by ransomware attacks, patient lives can be at risk. This threat is particularly acute for small, rural, critical access and 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 delayed surgeries, risking patient 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 patient 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
- Loss of intellectual property or other confidential information
- Lawsuits
- Regulatory penalties and
- Strained employee morale and burnout.

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, the industry is 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: adoption of digital consumer wellness and fitness technologies; remote care models; and accelerating consolidation of health systems and 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 technology that is becoming increasingly important in the healthcare ecosystem but lacking common cybersecurity protections.

Ways to Deal with the Threat: Cybersecurity Legislation

The committee is considering two healthcare cybersecurity bills – the *Healthcare Cybersecurity and Resiliency Act of 2026* and the *Rural Hospital Cybersecurity Enhancement Act*. While the HSCC Cybersecurity Working Group has not formally considered these bills for the purpose of public comment and advice, I can say broadly in my own estimation that they represent a welcome indication of the Committee's attention to this complex and evolving challenge. These bills read as complementary

guidance for: 1) structured coordination processes and objectives across the U.S. Department of Health and Human Services (HHS), the Cybersecurity and Infrastructure Security Agency (CISA), and the healthcare industry sector, and 2) specific, targeted assistance to the nation's most under-prepared, rural, and resource-constrained health providers.

I can also say there are some passages in the bills that we stand ready to help the committee improve with clearer language and context, such as, inter alia:

1. Direct HHS and CISA to involve the council in cybersecurity policy deliberations, threat information sharing, and incident response advisories to the community;

2. Clarify section 4 of the cyber resiliency act to require that the HHS delegate for internal and external cybersecurity coordination be designated at the deputy assistant secretary level or above with the appropriate authority to influence policy and programmatic decisions;

3. Ensure that grant funding is available to the broadest community of resource-constrained health providers, and include the ability to replace old and vulnerable medical devices that can no longer be protected from cyber threats; and

4. Avoid Congressionally-prescribed technical solutions such as "multifactor authentication" and "encryption". Technology is constantly evolving in ways that will change the meaning, implementation and effectiveness of technical products and methods. Prescriptions for

technical solutions are better left to evolving industry security frameworks that are already widely recognized and referenced.

How We Support the Sector: HSCC Resources and Policy Engagement

All of our work is systematically conceived and developed under our mission's north star – our Health Industry Cybersecurity Strategic Plan 2024-2025. The Strategic Plan provides the compass for the sector's programmatic initiatives for advancing the preparedness and resilience of the sector against cyber threats. The Plan is organized into 12 Implementing Objectives across the spectrum of cybersecurity functions and stakeholders, based on an assessment of major trends in the industry and their cybersecurity implications through 2029. These trends include industry consolidation, continued evolution in technology and methods of delivering care, geopolitical and climate instability and the attendant supply chain effects, and financial and workforce shortages among the resource-constrained. The Plan envisions progress as being able to characterize our nation's healthcare cybersecurity by 2029 in the following way:

Reflexive Cybersecurity	Secure Design & Implementation	C-Suite Ownership	Cyber Safety Net	Cyber Competence	911 Cyber Civil Defense
Both practiced and regulated healthcare cybersecurity is reflexive, evolving, accessible, documented and implemented for practitioners and patients.	Technology and services across the healthcare ecosystem is a shared and collaborative responsibility.	Healthcare C-Suite embraces accountability for cybersecurity as enterprise risk and a technology imperative.	Under-resourced health organizations are supported in the form of financial, policy and technical assistance ensuring cyber equity across the ecosystem.	Workforce learning and application is an infrastructure wellness continuum.	Ensures that early warning, incident response and recovery are reflexive, collaborative and always on.

It is notable when looking at the Strategic Plan that there is considerable thematic alignment between its Implementing Objectives and the two cybersecurity bills under consideration at today's hearing. In particular, we point to complementary themes in 5 of our 12 Implementing Objectives:

Objective 2: Simplify access to resources and implementation approaches for the adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, and data.
Objective 6: Increase utilization of cybersecurity practices / resources / capabilities by public health, physician practices and smaller health delivery organizations (e.g., rural health).
Objective 7: Increase incentives, development and promotion of health care cybersecurity-focused education and certification programs.
Objective 11: Increase meaningful and timely information sharing of cyber disruptions to improve sector readiness.
Objective 12: Develop mechanisms to enable "mutual aid" support across sector stakeholders to allow for timely and effective response to cybersecurity incidents.

These and the other 7 Strategic Plan Objectives guide the prioritization of our shared, cross-sector challenges and the member-driven workstreams to address them. See page 20 of The Plan for the complete list of Objectives. Below is a summary of a few of the resources that answer the call of the Strategic Plan and indeed, that of the guidance contained in the bills under consideration today.

Operational Resources and Policy Alignment

The following section discusses a few of the almost 40 leading practices and programmatic initiatives that HSCC produces - *by the sector for the sector* - as a free, public-domain library of guidance and toolkits. For the purpose of illustrating alignment with these bills, our resources are categorized using the broad themes of *Preparedness and Resiliency*, and *Rural Cybersecurity and Workforce*. These themes align provisions in the committee's legislation with the operational guidance in our publications and the many recommendations for appropriate government policy and programs to support our shared objectives. A number of these recommendations fall outside this committee jurisdiction but nevertheless constitute the holistic remedies we see as necessary for this cross-cutting challenge.

HSCC Cybersecurity Resource Theme: Cybersecurity Preparedness and Resiliency

- Health Industry Cybersecurity Practices (HICP) - The HICP 2023 is an update to the 2019 HICP publication developed jointly by HSCC and HHS. It provides executives, health care practitioners, providers, and health delivery organizations with best practices for managing cyberthreats to safeguard patient safety. The HICP subsequently informed the development of the consolidated Healthcare Cyber Performance Goals based on a joint HHS-HSCC assessment called the Hospital Cyber Landscape Analysis, which identified the vulnerabilities and threats most frequently resulting in damaging attacks against hospitals and assessed the hospitals' known capabilities for preventing damaging cyber incidents.

- Sector Mapping and Risk Toolkit (SMART) - The SMART Toolkit was our answer to the catastrophic ransomware attack on Change Healthcare, a company that provides critical services to a third of the nation's health system. The disruption resulted in major health systems and hospitals losing massive amounts of revenue daily due to suspended prior authorization, claims processing, pharmaceutical prescriptions and blocked electronic remittances. The SMART Toolkit provides templates to map major health system workflows and identify and measure systemic risk posed by third party technology, software, and communications services essential to those clinical, administrative and manufacturing workflows.
- Operation Vital Signs – Hosted by the HSCC and the Health Information Sharing and Analysis Center, "Operation Vital Signs" was the first national healthcare cybersecurity tabletop exercise, held virtually over two days in July 2026 and involving more than 500 participants representing approximately 120 organizations. The exercise was structured to examine both enterprise-level and cross-sector response and recovery, including the potential

effects of a widespread disruption on critical functions and patient safety. At the sector level, the exercise focused on collective impacts, coordination, shared resources, and the flow of information among health sector organizations, government agencies, associations, and other sector partners. The final After Action Report with lessons learned and recommendations will be published in November.

- Operational Continuity-Cyber Incident Checklist – This toolkit provides a flexible protocol for operational staff and executive management to respond to and recover from an extended enterprise outage due to a serious cyber-attack. Its suggested operational structures and tasks can be modified or refined according to an organization's size, resources, complexity and capabilities.
- Cybersecurity Information Sharing Best Practices – A guide for how healthcare organizations can establish, manage and improve cyber threat information sharing programs for their enterprise.

HSCC Cybersecurity Resource Theme: Rural Cybersecurity and Workforce

- On the Edge: Cyber Health of America's Resource-Constrained Health Providers – Through interviews with 42 senior executives of resource constrained healthcare institutions in 31 states, this report examines how these health care systems – small, rural, critical access, family clinics, skilled nursing facilities, FQHCs and many more across the country – are only marginally prepared for ongoing cyber threats to clinical care and operational liquidity. The report recommends forms of support those providers would need against stiffer cybersecurity regulatory requirements contemplated in the pending HIPAA Security proposed rule. What we found is that these providers face significant challenges in managing cybersecurity due to limited workforce and expertise, outdated systems, and insufficient funding. These resource-

constrained healthcare providers are aware of the cybersecurity measures needed but lack the resources to implement them. They express a critical need *for workforce augmentation, financial support, and partnerships to enhance cybersecurity and protect patient safety*. The Rural Hospital Cybersecurity Enhancement Act substantially addresses some of these recommendations. But ultimately, in addition to the need for innovative private sector initiatives, partnerships and market drivers, we cannot make progress in these areas without government funding.

- Cybersecurity for Clinician Video Training Series – This video training series totals 47 minutes among eight videos, explaining in easy, non-technical language what clinicians and students in the medical profession need to understand about how cyber attacks can affect clinical operations and patient safety, and how to do their part to help keep healthcare data, systems and patients safe from cyber threats. The free resource is available on YouTube and downloadable files from our website.
- SecureTexas Initiative – Conceived by the Texas Health Services Authority – the umbrella health information exchange service in Texas - and DirectTrust, a healthcare focused non-profit accreditation organization, the groundbreaking SecureTexas initiative combines healthcare cybersecurity assessment with practical implementation support and workforce development. Developed in response to Texas House Bill 300, SecureTexas provides healthcare facilities with an affordable pathway to achieve robust cybersecurity standards in alignment with the specifically-chosen Health Industry Cybersecurity Practices. This is ultimately intended to build the next generation of healthcare cybersecurity professionals. We see this as a template or beta test for wider national rollout of HICP implementation – indeed many other HSCC best practices - using policy support from the government through innovative funding and incentive models.

- Workforce Guide - The Workforce Guide is a tool kit for recruiting and retaining skilled cybersecurity workforce in the healthcare sector. It helps hiring managers and Chief Information Security Officers think about cyber workforce development as a continuum, from: 1) hiring students, to 2) transitioning IT staff to cybersecurity responsibilities; 3) developing and managing professional development programs for executive-track cybersecurity personnel; and 4) outsourcing critical functions not otherwise resourced within the enterprise.
- *In process* – Related to the above Workforce Guide, we are working on an "Apprenticeship Starter Kit (ASK)" which will guide enterprises on how to cultivate and retain cyber talent in the health industry and clinical environment through upskilling programs and mentorship.

Many more published leading practices are available on our website at https://healthsectorcouncil.org/hscc-publications/ and include healthcare-specific programs for: managing cybersecurity implications of artificial intelligence in healthcare; medical device security and model cybersecurity contract language between device manufacturers and health providers; third party supply chain management; coordinating enterprise cybersecurity and privacy functions; and executive and board level engagement in cybersecurity risk-prioritization and incident response, among others.

Policy and Program Recommendations for Government

Given the distressed state of healthcare cybersecurity, the HSCC believes that we cannot pursue a strategy on just one element or subsector in a broader healthcare ecosystem vulnerable 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 a combination of cybersecurity regulation, policy, and voluntary practices and partnership implemented across the healthcare ecosystem. Accordingly, the HSCC regularly offers recommendations for both Congressional and Executive Branch consideration. Our most recent set of recommendations was published last year and are currently being updated. In the meantime, the existing recommendations can be found on the HSCC website at https://healthsectorcouncil.org/government-partners-forward-path-2025-cyber-program-recommendations/.

These proposals are neither exhaustive nor rigid in their descriptions. Some are more notional, meant to stimulate creative discussion between government and industry about the form and implementation of initiatives that can measurably improve cybersecurity management across the health sector.

We have made these recommendations in hearings to this committee twice before, as well as in hearings held by Senate HELP and Homeland Security and Governmental Affairs. We hope these recommendations are being heard and germinated. Indeed, it is encouraging that many of these recommendations are substantially acknowledged and integrated in the cybersecurity bills before the committee and under consideration in today's hearing – the *Healthcare Cybersecurity and Resiliency Act of 2026* and the *Rural Hospital Cybersecurity Enhancement Act.* As the recommendations listed below align with elements of the bills under consideration they will also reference HSCC best practices and initiatives that support those provisions in the legislation.

HSCC Recommendations Aligned with Health Care Cybersecurity and Resiliency Act

Preparedness and Information Sharing

- Congress should support a long-term extension of the Cybersecurity Information Sharing Act (CISA) of 2015, which established the so-called "405(d) Program that authorized joint initiatives and publications between HHS and the industry sector, and provided protections from regulatory jeopardy to industry stakeholders as incentive for voluntary threat information sharing with the government.
- 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.
- 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 similarly 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".
- HHS should encourage health sector organizations to join and actively participate in Health-Information Sharing and Analysis Center (Health-ISAC) as part of a robust resilience strategy.
- 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.

- 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.

Financial Support and Incentives

- CMS reimbursement incentives: As incentivized in P.L. 116-321 – the HITECH Act amendments - if an institution demonstrates implementation of HICP, the NIST CSF, or other recognized security practices 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 that: participate in the Health-ISAC or other ISAO's; manage cybersecurity of legacy medical technology and replacement programs; and include cybersecurity 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.
- 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, and local support services can partner with FBI and CISA offerings to enhance health sector security.

- Workforce augmentation for needed cybersecurity skills can be funded at the federal and state levels for assistance such as: CISA technical support programs; 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/); and, state national guard assistance for cybersecurity incident response, and other programs.
- 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
  - Conduits to rural community leaders and health care providers to share information and resources.
- HHS should establish needs-based subsidy and incentive programs to help resource-constrained health systems participate in the Health-ISAC or other information and sharing and analysis organizations to improve situational awareness and threat preparedness.
- 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.

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

Incident Response and Recovery

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

- 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.
- Cyber-attack victim reporting requirements should be waived while an incident response is underway in the early stages of discovery and operational triage.
- 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.
- 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.
- 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.
- Partner government and industry research activities toward technical and operational efficiencies for effective incident response and continuity to ensure rapid return to health delivery operations following a severe cyber-attack.

Workforce Development

- 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.
- Fund and supplement federal and 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.
- 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.
- Map the NICE Framework's Work Roles and Job Descriptions to the HHS-HSCC Health Industry Cybersecurity Practices to bring better and clarity and uniformity to matching skills with job descriptions - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

Regulatory Reform

- The January 2025 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 should be reset or abandoned.
- 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.
- As recommended in Section 12 of the Cybersecurity Resiliency Act, HHS, CISA and other agencies must work together to streamline and unify incident reporting requirements across multiple agencies. These duplicative requirements generally provide little benefit to the security and resiliency of the sector and seemingly only serve the agencies' expectations to exercise their authorities. The reporting ostensibly is to enable agencies to intake, process, analyze and then advise the sector on actionable threat intelligence and remediation opportunities, but in practice those communications back to the sector are often late, irrelevant, and long overtaken by subsequent events.

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 is 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.

This concludes my testimony, thank you.

##