Testimony of

Greg Garcia
Executive Director

of the

Healthcare and Public Health Sector Coordinating Council
Cybersecurity Working Group

on

Aging Technology, Emerging Threats: Examining Cybersecurity Vulnerabilities in Legacy Medical Devices

Before the

United States House of Representatives

Committee on Energy and Commerce

Oversight and Investigations Subcommittee

April 1, 2025

Statement Summary

The Health Sector Coordinating Council Cybersecurity Working Group (CWG) is a government-recognized critical infrastructure industry council of more than 490 healthcare providers, pharmaceutical and medical technology companies, payers, health IT entities and government agencies. We partner to identify and mitigate cyber threats to health data and research, systems, manufacturing and most importantly patient care. The CWG membership collaboratively develops and publishes free healthcare cybersecurity leading practices and policy recommendations, and we produce outreach and communications emphasizing the imperative that ***cyber safety is patient safety***.

We are glad the committee is taking up the important issue of legacy medical device security. This is a complex issue, involving technical, operational and business interdependencies between manufacturers and health providers. And while cyber attacks involving medical devices more often use those devices as portals or jumping off points to other hospital network data and functions, rather than direct attacks on the devices themselves, we cannot ignore the many vulnerabilities in both new and legacy devices.

We cannot ignore how the broader healthcare system is the most targeted now of all critical infrastructure sectors, by both criminal gangs and nation states. This fact requires a more urgent effort on the part of the government to protect health systems that can't match the firepower of nation state cyber trade craft.

For our own part, the CWG has published 5 extensive cybersecurity practices that were negotiated between medical product manufacturers and health providers. These publications guide manufacturers and health systems on how to:

- To Design and build cybersecurity into medical devices from the ground up, rather than bolted on later
- To Manage the security of medical devices as they age in the clinical environment, recognizing that it is a shared responsibility
- To Write model terms and conditions into contracts for the sale and service of medical devices.
- To deliver simple, actionable and consistent cybersecurity vulnerability communications related to products or services.
- To Respond to and recover from cyber incidents that impact computer controlled medical manufacturing, known as operational technology.
- (Soon to come) To Safely and cost effectively patch and update devices while in use in the clinical environment.

While we continue to improve on these practices, cost and operational pressures among both manufacturers and health providers continue to complicate uniform implementation. But a key point to be made is that the health sector is an interconnected and interdependent ecosystem. We cannot address the security of our medical device manufacturing in a vacuum. We must also consider how health systems appropriately manage cybersecurity of devices. We must scrutinize the procurement of unregulated software and components that support medical devices and other networked systems. And the government needs to bolster its counter-espionage capabilities to protect America's critical infrastructure from nation-state cyber-attacks. So there are many moving parts. Fixing a flat tire won't do you much good if the steering column is loose and the oil warning light is broken.

I will summarize with recommendations relevant to the importance of medical device security:

First, we submitted to the Administration yesterday a policy statement, which I would ask be entered into the record. In it we recommend initiation of a consultative process between the health sector and the government that starts with the best practices we have developed – by the sector for the sector and jointly with HHS. This process would supplant one-way government regulation that presumes the best way to do things, with a more deliberative pathway toward eventual requirements for minimum cybersecurity accountability.

Such discussions could include, for example:

- Recommendations that CMS review bundled payments to more thoroughly account for the expense of medical devices and the need to keep devices patched and up to date against cyber threats;

- Development and enforcement of higher standards of “secure by design and secure by default” for otherwise unregulated third-party technology and service providers that sell into critical healthcare infrastructure and medical device manufacturers;
    - This recommendation involves our national effort to diagram essential medical workflows supported by critical third-party services and functions that can cause systemic risk and cascading damage to patient care and operational resiliency if they are disrupted. Such disrupted workflows can include medical device imaging, diagnostics and therapeutic services; and

- Finally, mobilization of a more reflexive government and industry intelligence, preparedness and rapid response capability is essential for cyber events at the federal, state, regional and local levels, particularly against resource-constrained health systems and connected medical devices.

Introduction

Chairman Palmer, Ranking Member Clarke, 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 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 high technology and financial services companies and industry groups. In all of these capacities, I am proud of my public service.

We appreciate the Committee's holding this timely hearing to examine health sector cybersecurity of medical technology. My testimony today will focus not on the technical or operational aspects of medical technology security – I will leave that to others on this panel – but on what the health sector and government are doing to strengthen the security and resiliency of the health system and its interconnected ecosystem of subsectors.

Today, I will cover 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;

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

Third**,** how we are addressing health sector cybersecurity with a holistic approach.

About the Health Sector Coordinating Council Cybersecurity Working Group

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 that has historical recognition promulgated in national policy. Together we identify and mitigate systemic 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.

The HSCC CWG is a volunteer organization with a growing list of 460+ 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.

Where the CWG is focused on 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 40 to 140 organizations across the health industry and government that develop cybersecurity best-practices and resources for various healthcare cybersecurity disciplines. These disciplines include health provider cybersecurity hygiene; supply chain cyber risk management; workforce development; incident response and operational continuity; and medical technology security, among many others.

With that cross-functional cybersecurity imperative in mind, since 2019 the CWG has published 28 best practices and guidance documents that address the many recommendations of a 2017 HHS healthcare cybersecurity task force of industry and government experts. Those 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 sound cybersecurity practices 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.

Cyber Threats, Vulnerabilities and Incidents

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. In 2017, the HHS Healthcare 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 the proper 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
- Reduced stock value.

Medical Device Security in the Healthcare System

Medical devices are a critical component within the overall healthcare ecosystem. Medical devices provide critical capabilities that enable clinicians to better and more efficiently diagnose and treat their patients. These medical devices also represent a potential vulnerability within the healthcare technology environment and may also be impacted when the healthcare technology environment is hit with a cyber attack. Medical devices have become increasingly connected, which provides the ability to provide improved and more efficient health services but also exposes them to additional risks.

From the health provider's perspective:

- Unlike in other sectors, healthcare data must be portable. Sensitive patient information must move between various medical providers, pharmacies, diagnostic facilities, and payers to facilitate proper patient care and payment for those services;
- Many healthcare facilities, such as hospitals, operate in environments that are accessible to the public, which adds to the vulnerability;

- The average patient bed has 15 supporting medical devices, and a 500-bed hospital could have 7,500 devices, many of which are over 8-10 years old and connect to a network that may not be protected or segmented from other systems or databases;
- Thousands of hospital-deployed medical devices are supplied by many different manufacturers with various levels of security and patching protocols. Devices may have unencrypted hard drives or common passwords set by the manufacturer that cannot be changed. Implementing compensating controls, or taking them offline for patches, updates or replacements is complicated. Further complicating health provider replacement programs are budget constraints and small operating margins;
- Correspondingly, a 33% decrease in Medicare Physician payments when adjusted for inflation results in less money for health systems to upgrade or replace aging medical technology;
- Hospitals thus can't afford to purchase new technology routinely due to declining reimbursements and poor margins;
- This causes risk as older, unsecured technology continues to be used;
- This includes devices no longer supported by manufacturers for various reasons, including that they can't get patches from 3rd party software vendors.

And from the device manufacturer's perspective:

- The lifecycle of a medical device is significantly different from other typical IT technology:
  - Medical Device = 7-10 years once purchased

    - Technology (computer, server, phone) = 3 years

- The design and approval process for medtech is also significantly different from other typical IT technology
    - Submissions to FDA for pre-market approval = ~10 years
    - Submissions for updates that "substantially equivalent" in functionality to an existing approved device = ~5-7 years
    - Most unregulated IT devices/tech (including some software used in medtech not under FDA regulatory umbrella) = 1-2 years
- The pricing of medical devices varies widely depending on the device
    - Conventional devices like surgical gloves and routine medical supplies are commodities in competitive markets with high volume and low margin
    - Advanced products (which typically have software and embedded IT tech – like pacemakers and MRIs) are much less competitive, and therefore much more expensive, with higher margins.

Given the above factors, there is regulatory and market fragmentation in the development, approval, acquisition and operational support of medical technology in the clinical environment.

While these observations point to reasoned concern about risks associated with the cybersecurity of medical devices, experience shows that cyber attacks do not typically occur against medical devices specifically but more frequently are the result of 3 prevalent attack methods:

- Social engineering, such as email phishing
- Unpatched vulnerabilities of technology directly facing the internet
- Third party compromise.

That said, any high risk vulnerabilities that are addressable through better product security and implementation practices should indeed be addressed - to reduce risk, protect patient safety, and maintain public confidence in our healthcare system.

We certainly appreciate the committee's interest in the cyber health of the millions of medical devices in the healthcare system that are used to diagnose, monitor and treat patients. The HSCC has spent considerable energy – tens of thousands of collective people hours – developing ways to address cybersecurity challenges inherent in medical device manufacturing and use. Our organizing principle is that technology used in the clinical environment must be secure by design, by default, by demand and by deployment. That makes it a shared responsibility of the manufacturers and the providers. A few points, however, illustrate the complexity of those imperatives:

Through an organizational structure of cross-sector task groups consisting of major healthcare provider systems and medical device manufacturers, the HSCC has since 2019 developed an extensive library of 28 resources and best practices which, if implemented across the sector, would measurably increase the security and resiliency across the sector. Several of these directly address the complexity of medical technology security and accountability. Following is a brief description of these medtech security publications which can be found at https://healthsectorcouncil.org/tag/secure-medtech/:

- **Medical Device and Health IT Joint Security Plan** – a guide for implementing "secure-by-design" and "secure-by-default" principles throughout the product lifecycle of medical devices and health IT solutions. This plan is in its second iteration and has also been used to provide a basis for assessing and improving cybersecurity maturity across the industry.
- **Managing Legacy Technology Security** - a comprehensive guide for medtech manufacturers and health providers to implement cybersecurity in legacy as a shared responsibility in the clinical environment and provides insights for designing future devices that are more secure.
- **Model Contract-Language for Medtech Cybersecurity** - a model contract based on common understandings and reasonable commitments for cybersecurity between health providers and medtech companies at time of sale and during clinical use of the technology.
- **Medtech Vulnerability Communications Toolkit** – provides medical device manufacturers with models for simple, actionable and consistent cybersecurity vulnerability communications related to their products or services.
- **Medical Product Manufacturer Cyber Incident Response Playbook** – a comprehensive guide for medical product manufacturers responding to cyber incidents impacting computer-controlled manufacturing.
- And one more on the way about how best to safely and cost effectively patch and update devices used in the clinical environment.

These publications present negotiated consensus among prominent manufacturers, industry experts, and providers about those cybersecurity management practices to which they agree they should be accountable. And while we continue to improve on implementation and effectiveness of those practices across the health sector, pressures will remain on resource prioritization among both communities, whether it be manufacturer considerations about costs associated with re-engineering, retooling, global third party component sourcing and security, regulatory delay and time to market, or hospital concerns about cybersecurity costs and complexity, attracting and retaining clinical staff, physical facility upkeep and regulatory compliance, and reduced reimbursement pressures.

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.

Overarching HSCC Cybersecurity Recommendation

Our most immediate recommendation, as submitted to the Administration this week, is that ***the Administration and health sector leaders coordinated by HSCC initiate a structured series of consultations and workshops 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 this month.

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.

Operationalizing the Recommendation

Whether claims processing, lab and blood management or other critical healthcare services we regularly and too often see examples of essential utilities undergirding our critical infrastructure that, if severely disrupted or disabled, 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.

1) Our first operational recommendation, which is now underway and soon to be released, is to ***support and operationalize national health infrastructure mapping and risk assessment*** to provide visibility to those critical services and utilities that support the many interconnected interdependencies across the healthcare ecosystem. 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 involves 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 expectation 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.

2) 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.

3) ***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 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. We call it a "Healthcare 911 Cyber Defense": so much of our health system and patient care depend on minutes, hours and days, not on months. Investing in a rapid response force against systemic attacks, using 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, would be 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 underserved, under-resourced health providers across the nation.

4) ***Invest in a cyber safety net for the nation's underserved 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. Next week, the HSCC will release its report and findings from 40 interviews with resource-constrained provider institutions 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" usually wins. 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 supplemented.

5) 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-level 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.

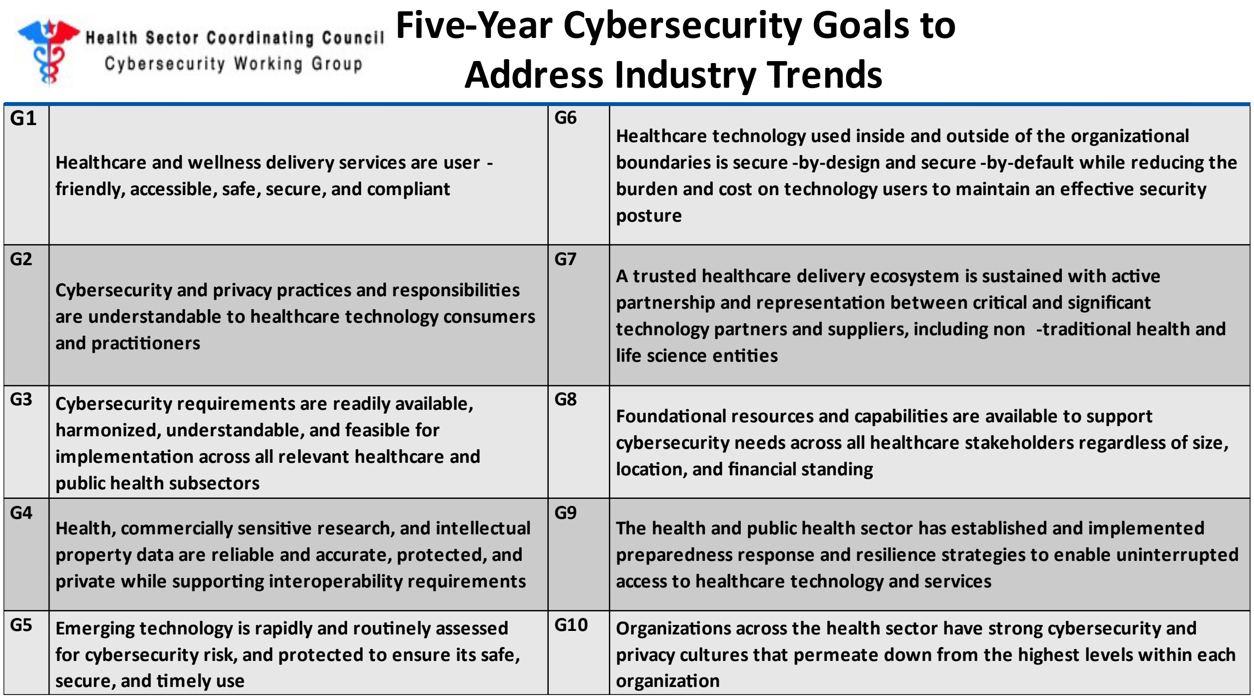
The strategic plan is meant for all HPH sub-sector participants, including medical device manufacturers (MDMs), pharmaceuticals, healthcare delivery organizations (HDOs), health insurance payors, regulators, and other industry and government participants whose products and services are used in healthcare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

The plan presents 10 end-state cybersecurity goals, with 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 that looks like:

- 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;
- Leaders in the healthcare C-Suite embrace accountability for cybersecurity as an enterprise risk and a technology imperative;
- A cyber safety net is in place to ensure that the weaker links in our interconnected ecosystem – those small, rural, critical access and other resource constrained health providers and local public health agencies – are able to ensure a minimum level of good cybersecurity to protect patient safety;

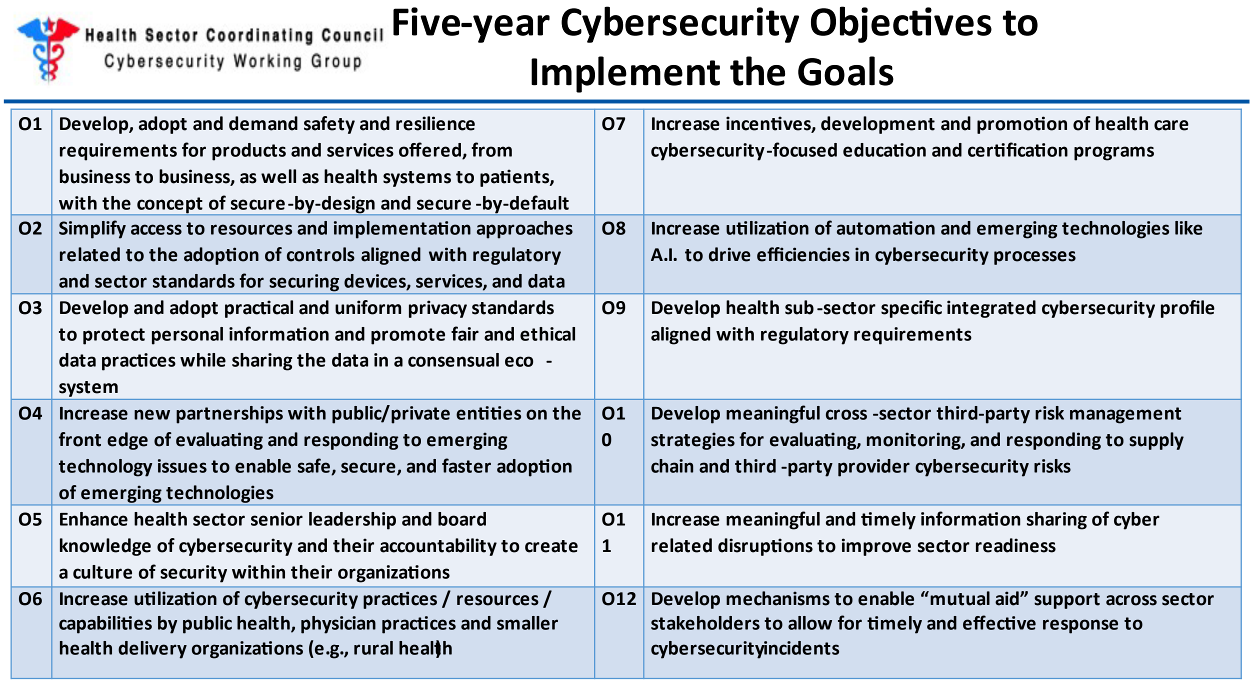
- Workforce cybersecurity learning and practice is a habit for healthcare infrastructure protection; and,
- A “911 Cyber Civil Defense” capability for community early warning, incident response and recovery is reflexive and always on.



Health Sector Coordinating Council
Cybersecurity Working Group

Five-Year Cybersecurity Goals to Address Industry Trends

G1	Healthcare and wellness delivery services are user - friendly, accessible, safe, secure, and compliant	G6	Healthcare technology used inside and outside of the organizational boundaries is secure -by-design and secure -by-default while reducing the burden and cost on technology users to maintain an effective security posture
G2	Cybersecurity and privacy practices and responsibilities are understandable to healthcare technology consumers and practitioners	G7	A trusted healthcare delivery ecosystem is sustained with active partnership and representation between critical and significant technology partners and suppliers, including non -traditional health and life science entities
G3	Cybersecurity requirements are readily available, harmonized, understandable, and feasible for implementation across all relevant healthcare and public health subsectors	G8	Foundational resources and capabilities are available to support cybersecurity needs across all healthcare stakeholders regardless of size, location, and financial standing
G4	Health, commercially sensitive research, and intellectual property data are reliable and accurate, protected, and private while supporting interoperability requirements	G9	The health and public health sector has established and implemented preparedness response and resilience strategies to enable uninterrupted access to healthcare technology and services
G5	Emerging technology is rapidly and routinely assessed for cybersecurity risk, and protected to ensure its safe, secure, and timely use	G10	Organizations across the health sector have strong cybersecurity and privacy cultures that permeate down from the highest levels within each organization



Health Sector Coordinating Council
Cybersecurity Working Group

Five-year Cybersecurity Objectives to Implement the Goals

O1	Develop, adopt and demand safety and resilience requirements for products and services offered, from business to business, as well as health systems to patients, with the concept of secure -by-design and secure -by-default	O7	Increase incentives, development and promotion of health care cybersecurity-focused education and certification programs
O2	Simplify access to resources and implementation approaches related to the adoption of controls aligned with regulatory and sector standards for securing devices, services, and data	O8	Increase utilization of automation and emerging technologies like A.I. to drive efficiencies in cybersecurity processes
O3	Develop and adopt practical and uniform privacy standards to protect personal information and promote fair and ethical data practices while sharing the data in a consensual eco - system	O9	Develop health sub -sector specific integrated cybersecurity profile aligned with regulatory requirements
O4	Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies	O10	Develop meaningful cross -sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third -party provider cybersecurity risks
O5	Enhance health sector senior leadership and board knowledge of cybersecurity and their accountability to create a culture of security within their organizations	O11	Increase meaningful and timely information sharing of cyber related disruptions to improve sector readiness
O6	Increase utilization of cybersecurity practices / resources / capabilities by public health, physician practices and smaller health delivery organizations (e.g., rural health	O12	Develop mechanisms to enable “mutual aid” support across sector stakeholders to allow for timely and effective response to cybersecurityincidents

The Cybersecurity Strategic Plan is the result of extensive and multiple collaborative sessions among almost 200 industry and government organizations across the HPH sector represented by senior cybersecurity and clinical executives and subject matter experts over a period of over 18 months.

Conclusion

Mr. Chairman, Members of the Committee, as a critical infrastructure industry the health sector and its dedicated workforce are mobilizing against the ongoing and existential threat of cyber disruption. We also recognize we need to move faster to keep up with the evolving threats. But through continued and expanded engagement in our collective purpose, broader awareness promotion, and forward-leaning government programs and support, we can move the needle and five years from now upgrade the healthcare cybersecurity diagnosis from "critical" to "stable condition."

Thank you.

Submitted for the record:

- Health Industry Cybersecurity Strategic Plan - https://healthsectorcouncil.org/the-plan/
- HSCC cybersecurity policy, programmatic and regulatory recommendations for government consideration - https://healthsectorcouncil.org/health-industry-cybersecurity-recommendations-for-government-policy-and-programs/