THE DEPARTMENT OF HEALTH AND HUMAN SERVICES

ADMINISTRATION FOR STRATEGIC PREPAREDNESS AND RESPONSE

Testimony before the
House Energy and Commerce Subcommittee on Oversight and Investigations

Hearing Titled
"Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies"

Brian M. Mazanec, PhD
Deputy Director, Office of Preparedness
Administration for Strategic Preparedness and Response

May 16, 2023

Chairman Griffith, Vice Chair Lesko, Ranking Member Castor, and distinguished members of the Committee, it is an honor to testify before you today on the Department of Health and Human Services' (HHS) efforts to strengthen the Healthcare and Public Health (HPH) critical infrastructure sector's preparedness for and response to malign cyber activity.

I am grateful for this opportunity to address this subcommittee and appreciate your continued support in this important area for national and health security. My testimony today summarizes (1) the growing cyber threat facing the HPH sector; (2) the role of HHS and the Department's Administration for Strategic Preparedness and Response (ASPR) as the Sector Risk Management Agency (SRMA) in addressing this threat; and (3) our current approach to strengthen the sector's cybersecurity today and into the future.

As you are all too aware, the HPH sector continues to experience an array of increasingly sophisticated cyberattacks that exploit complex, interconnected hospital infrastructures, historically underfunded cybersecurity functions, and an often-unwieldy number of vulnerable legacy systems and network-connected medical technologies, including medical devices. These cyberattacks against the HPH sector are growing both in numbers and severity, with the frequency of cyberattacks on hospitals and health systems more than doubling from 2016 to 2021.[1] Specific to ransomware, according to the Federal Bureau of Investigation's (FBI) Internet Crime Reports, the HPH sector experienced a 42 percent increase in ransomware attacks compared to 2021.[2] There are, on average, six or more significant cyber incidents impacting the sector every week. Ransomware is currently the largest threat to the HPH sector and the Administration has identified it as a key sector, alongside the transportation, banking, and water sectors.[3] The bad actors conducting these cyberattacks against the HPH sector generally have a few known motivations influencing their actions, including financially motivated crime; state-sponsored attacks for the purposes of exfiltration of sensitive information or to generate currency; and hacktivism to influence or inflict reputational impacts.

Cyberattacks directed at hospitals can impact patient care and safety, including extended disruptions caused by multi-week outages; patient diversion to other facilities; and strain on acute care provisioning and capacity, causing the cancellation of medical appointments, non-rendered services, and delayed medical procedures (particularly elective procedures). Further, a recent study reported data from an unaffected hospital geographically adjacent to an institution that had been hit by ransomware and found that the emergency room of the unaffected hospital had significant increases in the numbers of patients arriving for treatment, the number of ambulances diverting patients, the amount of time that patients waited to receive care, and an increase in time-sensitive, resource-intensive medical conditions like stroke requiring treatment.[4] This data demonstrates that cyberattacks against hospitals not only affect the targeted institution, but have "blast radius" effects on the surrounding region, similar to conventional disasters like earthquakes or hurricanes.

---

[1] *JAMA Health Forum.* 2022;3(12):e224873. doi:10.1001/jamahealthforum.2022.4873

[2] Federal Bureau of Investigation, *Internet Crime Report 2021,* and *Crime Report 2022*

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/

[4] https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585

A recent study from IBM reports that the average cost of health care cyberattacks averaged $4.35 million in 2022.[5] The average cost has climbed 12.7 percent since 2020, making health care cyberattacks the most expensive data breaches out of any industry.

ASPR Serves as the HHS Lead Sector Risk Management Agency for the Healthcare and Public Health Sector

ASPR's mission is to help the country prepare for, respond to, and recover from public health emergencies and disasters. A part of that responsibility as the SRMA, ASPR helps prepare the health care sector for disasters and emergency events through the Health Care Readiness and Recovery program.

In 2013, Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience established the federal government's strategy to protect the critical infrastructure that underpins American society.[6] PPD-21 defined 16 critical infrastructure sectors and identified specific agencies to support the management of threats and hazards faced by each sector, including the HPH sector. The 2021 National Defense Authorization Act then codified core responsibilities for each of these lead agencies, redefining them as SRMAs. HHS is the designated SRMA for the HPH sector, responsible for providing specialized sector-specific expertise and supporting programs and associated activities for the sector.

As directed by HHS, ASPR carries out this SRMA function through our Office of Critical Infrastructure Protection within our Office of Preparedness. ASPR coordinates regularly with our colleagues across HHS, including the Food and Drug Administration (FDA), the HHS 405(d) Program and Health Sector Cybersecurity Coordination Center (HC3) within the Office of the Chief Information Officer (OCIO), the Office for Civil Rights (OCR), the Office of the National Coordinator for Health Information Technology (ONC), the Centers for Medicare & Medicaid Services (CMS), and the HHS Office of the Inspector General (OIG), to name a few.

Working as a team, all HHS agencies and divisions bring together their unique cybersecurity perspectives, expertise, and authorities as a single collaborative effort to assist the HPH sector, from direct engagement with the HPH sector on cybersecurity activities to collaborative regulatory actions with the goal of HPH sector protection. For example, OCR collaborates with ONC on development of and enhancements to the Security Risk Assessment (SRA) Tool that provides small- and medium-sized HPH sector organizations a tool to identify and assess security risks to health information within their organizations. HHS is best positioned to serve as SRMA for the HPH sector, as we leverage existing relationships in the regions and with HPH sector partners and utilize our resident expertise in the Department.

HHS—in Coordination with Key Partners—is Working to Strengthen the Cybersecurity of the Healthcare and Public Health Sector

---

[5] IBM, *Cost of a Data Breach 2022 Report;* *https://www.scmagazine.com/analysis/ransomware/scripps-health-cyberattack-ehr-downtime-caused-112-7m-in-lost-revenue-recovery#*

[6] *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*, February 12, 2013

HHS—with ASPR coordinating in its SRMA role, coupled with active involvement from other stakeholders across the Department—is undertaking numerous proactive measures to ensure we are well-positioned to address these growing cyber threats and strengthen the HPH sector's cybersecurity posture. SRMA responsibilities involve activities focused on sector risk management and assessing sector risk; sector coordination; facilitating information sharing; supporting incident management; and contributing to emergency response.

Developing Resources and Supporting Risk Mitigation Activities

HHS—jointly with our interagency and private sector partners—creates detailed resources and materials for the sector providing best practices and recommendations for building and maintaining cyber resilience and preparedness. HHS recently published the 2023 edition of the Health Industry Cybersecurity Practices (HICP), the Hospital Resiliency Landscape Analysis, and the Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide. HHS now offers free cybersecurity training and resources on its website through an education platform called "405(d)'s Knowledge on Demand" and ASPR's Technical Resources, Assistance Center, and Information Exchange (TRACIE), which provides online technical resources on health care cybersecurity. These resources are widely distributed and utilized; for example, in the first week of release, the 2023 version of the HICP had over 7,600 downloads and the Hospital Resiliency Landscape Analysis had over 6,800 downloads. HHS also collaborates with federal partners to provide actionable, credible threat intelligence to the sector to help it better strengthen the security posture of the HPH infrastructure. The HHS Office of National Security, HC3, and ASPR work together, along with our interagency partners, on identifying, collating, and analyzing threat intelligence. For example, over the past three years, HC3 has released over 190 products to support the HPH sector, including alerts, threat actor profiles, and threat briefings. HHS also recommends a Department of Homeland Security (DHS)-created cybersecurity checklist and primer as well as a no-cost Cyber Resilience Review, which is a voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices.

Facilitating Sector Coordination

HHS leverages these previously mentioned resources and closely coordinates and collaborates on cyber-related initiatives intended to strengthen the HPH sector's cybersecurity posture with DHS' Cybersecurity and Infrastructure Security Agency (CISA) and other relevant federal departments and agencies; with critical infrastructure owners and operators; with independent regulatory agencies where appropriate; and with State, local, tribal, and territorial (SLTT) entities. OCR, FDA, OCIO, ONC, ASPR, and other HHS divisions work closely with the HPH sector through the Healthcare Sector Coordinating Council (HSCC) by collaborating with peers in the private sector to develop and publish resources and best practices on protecting the HPH sector, including documents on securing legacy devices and implementing a cybersecurity framework. For example, we coordinate with over 15 government and over 300 private sector partner organizations via the HSCC Joint Cybersecurity Working Group—which has 16 active task groups—to align security approaches, assess risks and share mitigation measures.

Internal to HHS, ASPR manages the HPH SRMA Cyber Working Group, which brings together cyber experts from across HHS each week to coordinate HHS activities related to private sector coordination and to address critical information requests and policy issues identified internally or by HHS leadership, CISA, the National Security Council, and the Office of the National Cyber Director. These efforts are part of the larger HPH sector efforts, supporting and being supported by the broader all-hazards Sector Coordinating Council and Government Coordinating Council.

Leading Response Planning and Supporting Incident Response

Response planning for cyber incidents is critical as the frequency and intensity of these attacks increase. HHS recently completed a *Healthcare and Public Health Sector Risk Management Agency Cyber Incident Response Plan*, which provides the framework to coordinate processes for HPH sector cyber incident management within HHS. HHS is also developing a public-private sector partnership playbook to promote collaboration during all-hazards events, including cyber events. HHS has engaged with CISA and other sector partners to support over a dozen tabletop exercises to improve sector incident responses process and procedures. During these exercises, HHS provides subject matter expertise on how the entity could be better prepared—for example, by advising an entity to include a communications plan for how to engage staff and the public on the incident and expectations for recovery.

In responding to actual cyber incidents facing the HPH sector, HHS reaches out to over 8,000 government and private sector partners across the sector during cybersecurity incidents to inform response operations and mitigate impacts to patient care. From January 1, 2023, to May 8, 2023, we triaged 69 cybersecurity incidents, working closely with CISA and the Federal Bureau of Investigation (FBI) and conducting outreach to multiple organizations for information and data analyses to determine potential impacts to patient care and safety. We work closely with our FBI and CISA colleagues to identify technical information that can be shared with the private sector and providing actionable intelligence to them so they can evaluate their systems to eliminate or mitigate related vulnerabilities.

Utilizing Regulations to Enhance Cybersecurity

HHS also has a regulatory role over certain elements of the HPH sector, and this role helps strengthen the sector's cyber posture. OCR administers and enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules. The HIPAA Security Rule establishes national standards to protect electronic protected health information (ePHI) created, received, maintained, or transmitted by HIPAA-regulated entities. The Security Rule requires appropriate safeguards to ensure the confidentiality, integrity, and availability of ePHI. Further, regulated entities that can adequately demonstrate that recognized security practices—such as the current version of the HICP and the Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide—have been in place for the previous twelve months or more may be able to mitigate certain penalties following a cyber incident.

With respect to medical devices, the FDA clears, authorizes, and approves devices to be marketed when there is a reasonable assurance that the devices are safe and effective for their intended use, which includes the cybersecurity of such devices. FDA provides guidance

regarding the cybersecurity expectations of medical devices for medical device manufacturers, which is also useful for health care delivery organizations as they review their management of medical device cybersecurity. Additionally, section 3305 of the Consolidated Appropriations Act, 2023 granted FDA additional statutory authority to provide for the reasonable assurance of cybersecurity within medical devices, by requiring that medical devices meet select cybersecurity requirements.

Challenges Going Forward

HHS is working diligently to strengthen cyber security and address the impacts of cyberattacks on the health care system. As we move forward, there are additional authorities and resources that would advance ASPR's ability to fully implement its plan to bolster HHS's cyber SRMA activities. For example, we are in the process of establishing a dedicated Cyber Division within ASPR's Office of Critical Infrastructure Protection. If ASPR is granted direct hire authority, as requested through the Pandemic and All-Hazards Preparedness Act (PAHPA) reauthorization process, we would be able to bring critical staff with cyber expertise into the organization more quickly and move forward to address challenges without delay. We would also be better positioned to immediately expand and enhance our efforts as the SRMA lead for the HPH sector. Additionally, we are looking to establish a new HHS cyber incident ticketing system to better track incidents and strengthen threat intelligence sharing through embedded liaisons within CISA and the FBI. Dedicated resources are needed to implement and operate supporting systems, as included in the FY 2024 President's Budget request. We continually assess and identify whether any additional authorities are needed to support our role as SRMA for the HPH sector, and I look forward to working with all of you if any other needs arise.

Conclusion

As increasingly sophisticated and pervasive cyber threats continue to grow and evolve, ASPR remains committed to executing its SRMA responsibilities to prepare for and respond to cyber threats in the HPH sector. Thank you again for inviting me to testify before you today. I look forward to answering your questions and working with you and your staff to strengthen the cybersecurity of the HPH sector.