House Committee on Energy and Commerce
Oversight & Investigations Subcommittee Hearing
"Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies" May 16, 2023

Questions for the Record submitted for Brian Mazanec, Ph.D., Deputy Director, Office of Preparedness, Administration for Strategic Preparedness and Response, Department of Health and Human Services

The Honorable H. Morgan Griffith

1. Late last year, the Cybersecurity Infrastructure & Security Agency (CISA) released its new Cross-Sector Cybersecurity Performance Goals (CPGs), a foundational set of information technology and operational technology practices and recommendations intended to help smaller, lesser-resourced organizations better prioritize cybersecurity efforts and reduce risk. It is the Committee's understanding that CISA stated at the time that it was going to work with Sector Risk Management Agencies (SRMAs) to develop sector-specific CPGs.

    a. **Has the Department of Health and Human Services (HHS) engaged CISA on developing these sector specific CPGs, and if so, how are those efforts progressing? When should we expect them to be done?**

    Response: In 2017, HHS published the Health Industry Cybersecurity Practices (HICP) document that identified key threats and mitigation practices specific to the Healthcare and Public Health Sector. This document was refreshed and published in April 2023 with updated information acknowledging the changes in the sector and threats since 2017. As one of the cornerstone documents for health care cybersecurity, the HICP is becoming widely acknowledged and implemented by the HPH Sector as evidenced by the data outlined in the Hospital Resiliency Landscape Analysis.

    Related to the development of CPGs, in March 2023, CISA published an update to the CPGs. The CPGs are intended to be a baseline set of cybersecurity practices broadly applicable across critical infrastructure. The CPGs provide a prioritized set of security practices for information technology (IT) and Operational Technology (OT) owners. The CPGs were a direct response to the challenge identified in National Security Memorandum (NSM)–5: *Improving Cybersecurity for Critical Infrastructure Control Systems* to develop baseline cybersecurity goals that are consistent across all critical infrastructure sectors. HHS is currently coordinating with CISA to ensure that all sector-specific CPGs are aligned in intent and messaged in a consistent manner with the HICP and other sector-specific resources to reduce confusion or fatigue within the HPH Sector. Coordination activities between CISA and HHS on this initiative is in the early stages.

    b. **How is HHS using CISA's cross-sector CPGs to drive security improvements in the healthcare and public health sector?**

    Response: In 2017, HHS published the Health Industry Cybersecurity Practices (HICP) document that identified key threats and mitigation practices specific to the Healthcare and Public Health (HPH) Sector. This document was refreshed in 2023 with updated information acknowledging the changes in the sector and threats since 2017. As one of the cornerstone documents for health care cybersecurity, the HICP is widely acknowledged by the HPH Sector. Due to the existence of the HICP and the overall consistency between the HICP and the CPGs, the HPH Sector continues to rely primarily on the specialized HICP document to provide specific recommendations to the sector.

2. **How do you measure and report on the impact and outcomes of your cybersecurity initiatives and investments on cyber-physical systems in critical infrastructure?**

   Response: To support development of a baseline of cyber capabilities across the sector, HHS recently released the Hospital Resiliency Landscape Analysis in April 2023. This document was developed in partnership with the Health Sector Coordinating Council (HSCC) and includes an identification of the biggest threats facing hospitals as well as an assessment of cybersecurity capabilities relative to commonly accepted cybersecurity practices. This document also offers a window into how the sector is adopting and implementing the cybersecurity best practices as outlined by HICP. While early and limited in scope, this iteration of the Landscape Analysis is a baseline and we are in early discussions on how to expand and build upon this effort. HHS sees this analysis as a fundamental way we can measure the impact and outcomes of our efforts.

   In parallel, ASPR is developing version 2.0 of the Risk Identification and Site Criticality Toolkit (RISC Tool), which supports an all-hazards, objective, data-driven risk assessment for the HPH Sector. The RISC Tool includes an assessment on cybersecurity, closely aligning to the NIST Cybersecurity Framework. Version 2.0 is planned to launch in the fall of 2023 and will provide a source of data to HHS for measuring impact and outcome of activities through the analysis of voluntary self-reported risk assessment data.

   Lastly, within the HPH Sector Joint Cybersecurity Working Group, there is Measurement Task Group focused on understanding current state and changes in cybersecurity posture within the HPH Sector. Though this Task Group's work is still in its nascent stage, it will help drive strategies and activities to measure progress across the sector with respect to cybersecurity.

3. **What are the main challenges and gaps that hinder effective collaboration and information sharing between SRMAs and private sector stakeholders on cyber-physical threats and incidents, and what are you doing to address them?**

   Response: HHS is working diligently to strengthen cybersecurity 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 in the FY 2024 President's Budget, we would be able to bring critical staff with cyber expertise into the organization more quickly and move forward to directly support and aid preparedness, response, and recovery activities 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. A key limitation on the ability for sector entities to share information with the government is the fear of litigation from customers, we have heard from sector stakeholders that this is a key reason for not sharing information. Additionally, sector stakeholders need additional reassurance that information shared with the department for security sharing purposes is not then used for regulatory reasons.