Health Sector Coordinating Council
Cybersecurity Working Group

Health Sector Cybersecurity Working Group

Testifies to House Energy and Commerce Committee

with Recommendations for Preventing Future Catastrophic Cyber Attacks

Washington, D.C., April 16, 2024 - Today, the Healthcare and Public Health Sector Coordinating Council (HSCC) testified on a panel to the House Energy and Commerce Subcommittee on Health about the aftermath of the Change Healthcare cyber attack on the nation's health systems, and how to prevent future disruptions of such magnitude.

HSCC Cybersecurity Working Group (CWG) Executive Director Greg Garcia told the committee that "the Change Healthcare attack that occurred on February 21 imposed a stark reminder to the health sector – and indeed every critical industry sector – that there are 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." Garcia added, "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."

The CWG Executive Director went on to make several recommendations for industry and government action:

- Perform a health infrastructure mapping and risk assessment. This will provide visibility to those critical services and utilities – such as Change Healthcare - that support the many essential dependencies across the healthcare ecosystem.
- Assess consolidation proposals for mergers and acquisitions against their potential for increased cyber incident and impact risk.
- 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.
- Invest in a government-industry rapid response capability.
- Invest in a cyber safety net for the nation's underserved providers, built on accountability and incentives**.** This includes testing the effectiveness of an HHS budget proposal blending incentives and accountability modeled after the Promoting Interoperability Program. It calls for an $800 million commitment over two years to certain high-need hospitals to implement baseline "cyber performance goals." After that, penalties will apply to those that don't meet those minimum standards.
- Finally, over the next five years, the industry must implement *the HSCC 5-year Health Industry Cybersecurity Strategic Plan.* The plan recommends 10 end-state cybersecurity goals, and 12 implementing objectives to achieve those goals by 2029.

"If we make progress against the goals and objectives," Garcia said, "we can achieve an overall industry target state that looks like:

- Healthcare cybersecurity is made easier for practitioners and patients;
- Secure design and implementation of technology and services is a shared and collaborative responsibility;
- Leaders in the healthcare c-suite own cybersecurity as an element of enterprise risk;

- A cyber safety net is in place to promote cyber equity across small, medium and large entities;
- Workforce is trained in good cybersecurity; and,
- A "911 cyber civil defense" capability to lead incident response and recovery is reflexive and always on."

Garcia concluded his testimony with a challenge to the Sector: "The health industry must be sensitized to the imperative that cyber safety is patient safety. All healthcare stakeholders – that means providers, payers, medical technology and health IT, pharmaceuticals, public health, and government - are responsible for cyber safety, so that our nation's clinicians can do their job."

The HSCC CWG prepared statement can be downloaded from
https://healthsectorcouncil.org/HouseTestimony

More information: *https://healthsectorcouncil.org/contact/*