HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership

June 9, 2021

The Honorable Joseph Biden
President of the United States
Washington, DC 20500

Dear President Biden:

As a national critical infrastructure designated by the U.S. Department of Homeland Security, the healthcare sector faces an urgent need to strengthen the cybersecurity of healthcare and public health data, medical technology and information technology systems. The Healthcare and Public Health Sector Coordinating Council (HSCC) was pleased to see that the recently enacted American Rescue Plan directs $650 million to CISA for cybersecurity risk mitigation programs, though none directly targeted for the healthcare sector. In assessing how the American Rescue Plan, coupled with the recently released Executive Order on Improving the Nation's Cybersecurity, can measurably strengthen the security and resiliency of the healthcare system and patient safety, we request an enhanced strategic planning process with the Administration that will complement the ongoing cybersecurity partnership between the HSCC, the Department of Health and Human Services and other essential government partners.

The HSCC is a private sector-led critical infrastructure advisory council organized under PPD-21 and preceding executive orders, representing large, medium and small health industry stakeholders working with government partners to identify and mitigate threats and vulnerabilities affecting the ability of the sector to deliver healthcare services to our nation's citizens. A major component of the HSCC is its Cybersecurity Working Group, which represents more than 300 healthcare organizations in direct patient care; medical materials; health information technology; health plans and payers; laboratories, biologics and pharmaceuticals; and public health. Our members collaborate to improve the cybersecurity and resiliency of our healthcare systems and in so doing protect patient safety.

The healthcare industry faces relentless cybersecurity threats that have grown in magnitude and complexity year after year. These threats to the technology that is integral to patient care have worsened over the course of the pandemic, especially in the proliferation of ransomware attacks. One study found a 55% jump in cyber incidents against our sector in 2020.[1] According to a joint bulletin authored last October by the DHS Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Department of Health & Human Services (HHS), and the Federal Bureau of Investigation (FBI), there was credible information of increased and imminent ransomware threats to our sector. This was quickly followed by the SolarWinds network management threat identified in an emergency directive by CISA and then another related to

[1] Healthcare Cyber Attacks Rise by 55%, Over 26 Million in the U.S. Impacted - CPO Magazine

Microsoft Exchange Servers. A quick internet search the first week of May reveals several hospitals being taken down by cyber-attacks.

Cybersecurity incidents are a threat not only to national security, they also jeopardize patient safety, as attacks can cause denial of service, medical device corruption, and data manipulation that directly impact clinical operations, patient care and public health. In addition, healthcare data and information remain lucrative targets for theft and exploitation, particularly through ransomware attacks and COVID-themed social engineering by criminal groups and adversarial nation states.[2] A series of recent bulletins testifies to these threats.[3]

Phase I of the Administration's infrastructure plan calls for increasing "resilience in the most essential services, including the electric grid; food systems; urban infrastructure; ***community health and hospitals (emphasis added)***; and our roads, rail, and other transportation assets." We urge that a future phase of the plan include a planning process with the health sector to focus policy and resources on specific programs that will facilitate a collaborative, public-private partnership to strengthen healthcare cybersecurity.

The HSCC has made tangible progress toward recognizing and addressing numerous weaknesses in the cybersecurity of our systems, operations and supply chain, particularly through industry-developed best practices and guidance developed (some jointly with HHS and FDA) over the past three years. These include resources on: medical device product security and management; industry/HHS-developed cybersecurity practices for health delivery organizations (a mandate of §405(d) of the Cybersecurity Act of 2015) based on the NIST Cybersecurity Framework; cybersecurity management of healthcare supply chains; telehealth cybersecurity; and protection of innovation capital such as vaccine research against cyber theft.

These initiatives stem from recommendations made in 2017 by the HHS-appointed Health Care Industry Cybersecurity (HCIC) Task Force, which pointed to the need for more coordination of healthcare cybersecurity planning and resources between industry and government, particularly toward incentivizing industry investment with government support; building security into healthcare software and technology; workforce training; improvement of information sharing and incident response; and others. As the resulting best practices by the HSCC align with the aims of both the software and technology security recommendations of Section 4 of the Executive Order on Improving the Nation's Cybersecurity and the HCIC Report, we believe that an accompanying investment through the American Rescue Plan toward a structured healthcare cybersecurity partnership will amplify our efforts and help drive a culture of security and resiliency to a health sector that is otherwise stretched to its limits to meet its clinical and public health obligations.

We note with interest the President's recent initiative aimed at hardening our nation's electric power system against cyber threats. We believe an analogous effort for the health sector would

[2] PowerPoint Presentation (hhs.gov)
[3] NCSC_China_Genomics_Fact_Sheet_2021.pdf (dni.gov), 20201222-001_FBI PIN.pdf (govdelivery.com)

strengthen collaboration and resolve across the sector, especially following a year in which our sector and country fought the pandemic and multiple cybersecurity threats simultaneously. The Colonial Pipeline ransomware attack, the power outages resulting from the winter storms experienced in Texas earlier this year, and the impact the long-term lack of electricity had on hospitals, COVID-19 treatment and COVID-19 vaccination, are stark reminders of how interconnected the healthcare sector is with other critical sectors like power, water and communications, and how robust cybersecurity management is critical to the operational continuity and resiliency of our national critical functions.

As you lead the nation out of the pandemic, put more Americans back to work and increase their access to health insurance, the ability of the healthcare sector to deter cyber threats is imperative for the nation to maintain public health and global competitiveness beyond the pandemic.

The healthcare sector, despite making progress over the past several years, has struggled to keep up with the onslaught of cyber threats without enhanced federal programs and engagement. We are particularly concerned that lesser resourced organizations, such as small and medium sized healthcare providers and critical access hospitals, continue to fall further behind. We are only as strong as the weakest link, and it benefits the entire sector when we can improve every entity's cyber resilience.

We appreciate the opportunity to share our recommendation that future infrastructure plans support healthcare cybersecurity infrastructure, and hope to engage in a focused discussion with your team about our shared objectives.

Sincerely,

Michael Wargo *RN, BSN, MBA, PHRN, CMTE*
Chair, U.S. Healthcare and Public Health Sector Coordinating Council (HSCC)

Greg Garcia
Executive Director
HSCC Cybersecurity Working Group

cc:

The Honorable Nancy Pelosi
Speaker
U.S. House of Representatives
Washington, DC 20515

The Honorable Chuck Schumer
Majority Leader
U.S. Senate
Washington, DC 20510

The Honorable Kevin McCarthy
Republican Leader
U.S. House of Representatives
Washington, DC 20515

The Honorable Mitch McConnell
Minority Leader
U.S. Senate
Washington, DC 20510