

Congress of the United States
Washington, DC 20515

August 11, 2022

The Honorable Xavier Becerra
Secretary
Department of Health and Human Services (HHS)
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Secretary Becerra,

The COVID-19 pandemic revealed systemic challenges facing the healthcare and public health (HPH) sector. Early shortages of personal protective equipment demonstrated the challenges of supply chains dependent on adversarial foreign nations. Demands placed on healthcare workers exacerbated workforce challenges particularly in underserved and rural communities. For those of us working on issues of national cyber resilience, COVID-19 was accompanied by another epidemic – that of ransomware.

Ransomware attacks on the HPH sector have skyrocketed in the past two years as opportunistic criminals recognized that hospitals may pay quickly to resolve issues and protect patient safety. Meanwhile, the troves of personally identifiable information and personal health information make organizations in the sector valuable targets for both criminal and nation-state hackers.

Against this backdrop, we were heartened to see the White House host an executive forum on healthcare cybersecurity and the recognition by your Department and the other participants of the importance of improving the cybersecurity of this vital critical infrastructure sector. We also appreciate the FDA's prioritization of medical device cybersecurity and the growing ability of the Department's Critical Infrastructure Protection Division and the Health Sector Cybersecurity Coordination Center (HC3) to explain cyber threats through a sector-focused lens.

We remain concerned, however, about the lack of robust and timely sharing of actionable threat information with industry partners and the need to dramatically scale up the Department's capabilities and resources. With cyber threats growing exponentially, we must prioritize addressing the HPH sector's cybersecurity gaps.

As former co-chairs of the Cyberspace Solarium Commission, and authors of the Sector Risk Management Agency (SRMA) legislation now in use, we recognize the important partnership between the executive and legislative branches to properly organize and resource public-private

collaboration to protect against cyber threats. Thus, we are requesting a briefing from your office on the status of efforts to strengthen the department's capabilities as the SRMA and to operationalize collaboration with the organizations throughout the sector.

As part of this briefing, we would appreciate an assessment of:

- the current organizational structure and roles and responsibilities that HHS employs to support HPH cybersecurity and serve as the SRMA for the entire HPH. including intra-Department coordination (e.g. how the Administration for Strategic Preparedness and Response serves as the SRMA coordinates with the Chief Information Officer which leads the HC3);
- the current authorities HHS has to improve cybersecurity of the HPH sector as well as the gaps in those authorities and what more might be needed to ensure HHS has the authorities it needs;
- the resources – including personnel and budget – that HHS requires to serve as an effective sector risk management agency;
- the interagency coordination structures, successes, and challenges utilized to support HHS's efforts and HPH cybersecurity efforts.

We and our colleagues can only conduct effective oversight if we understand the challenges that your department and the HPH sector are facing. As such, as part of the briefing, I would welcome an unclassified threat briefing from your office on the cybersecurity risks to this most vital critical infrastructure sector.

Thank you for your attention to this important issue. I look forward to working with you to improve the cybersecurity of the healthcare and public health sector and, by extension, make our nation more resilient in cyberspace.

Sincerely,



ANGUS S. KING, JR.
United States Senator



MIKE GALLAGHER
Member of Congress