United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

March 25, 2024

The Honorable Xavier Becerra
Secretary
U.S. Department of HHS
Independence Ave, S.W.
Washington, D.C. 20201

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security
245 Murray Lane
Washington, D.C. 20528

Dear Secretary Becerra and Director Easterly,

I write to request that the Department of Health and Human Services (HHS) and the Cybersecurity and Infrastructure Security Agency (CISA) prioritize protecting Americans from cyberattacks in the health care sector. The recent cyberattack on a UnitedHealth Group subsidiary, Change Healthcare, has disrupted their ability to process medical claims, impacting millions of Americans trying to fill their prescriptions and access health care services. Not only is this cyberattack impacting Americans domestically, but it has also disrupted access to health care on American military bases worldwide.

As the sector risk management agency for the health care sector, HHS is a critical resource and regulator for the victims of this attack and the healthcare ecosystem at large. Therefore, I request that HHS expand its technical cybersecurity guidance and increase engagement with private sector entities in the 405(d) Program and Task Group efforts and call on the Administration for Strategic Preparedness and Response (ASPR) to include the operational resiliency of the health care sector's platforms in the National Infrastructure Protection Plan. HHS should heavily encourage health care entities impacted by the attack to take advantage of available technical and financial resources and assistance from CISA, CMS, and other organizations.

I recognize the significance of the released Healthcare and Public Health Sector-specific Cybersecurity Performance Goals as a first step by HHS and applaud the work that has gone into encouraging the health care sector to invest in cybersecurity. It is absolutely critical that HHS prioritize measuring the implementation of its goals and publish minimum cybersecurity requirements. These sector requirements and goals should be aimed at supporting the facilities most at risk of cyberattack and should be enforceable through available mechanisms like the Centers for Medicare & Medicaid Services (CMS) Conditions of Participation for consistently low-performing hospitals. Without rapid measurable improvements in cybersecurity across the health care sector, incidents like this one will continue to impact patient outcomes and lead to significant financial, administrative, and logistical costs for health care facilities.

Public outreach and engagement are an important part of increasing cybersecurity across the health care sector. CISA and HHS in coordination should conduct a campaign to engage and inform health care entities and the public of cybersecurity best practices and resources available to them.

This campaign should also highlight guidance and information on the threat of ransomware attacks to the health care industry. CISA should also make available additional resources to the health care community, including technical resources, to ensure that the health care ecosystem is better equipped to mitigate cybersecurity threats and rapidly improve their cybersecurity to prevent future incidents.

I urge HHS and CISA to act expeditiously to ensure that these resources are provided to hospitals and health care systems, and to reduce the impact on patients and providers across the country.

As HHS and CISA work to support recovery efforts after this attack, I request your responses to the questions below:

1. As the Sector Risk Management Agency, what are the next steps HHS is taking to prevent another cyber incident like this from occurring?

2. How is HHS measuring and encouraging the implementation of its sector-specific cybersecurity performance goals?

3. What assistance did HHS offer to the impacted entities in the health care sector? Is HHS monitoring for the effectiveness of this assistance?

4. What kind of assistance, both technical and non-technical, did CISA offer to HHS during the incident and in the weeks after the incident?

5. To what extent did CISA share information on cyber threats to the health care sector with HHS and health care entities in the several months prior to the attack? What information was shared during and after the incident?

6. How is HHS coordinating with CISA to receive and distribute threat indicators, warnings, and indicators of compromise across entities in the health care sector? How is HHS and CISA measuring usage of these messaging services in the health care sector?

7. What assistance is CISA offering to impacted entities in the health care sector and how is CISA ensuring that entities are aware of the assistance?

Sincerely,

Gary C. Peters
Chairman
Committee on Homeland
Security and Governmental
Affairs

cc: Dawn O'Connell, Assistant Secretary, Preparedness and Response, Department of Health and Human Services
Lt. Gen. Telita Crosland, Director, Defense Health Agency
The Honorable Harry Coker, Jr, National Cyber Director, Office of the National Cyber Director