BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

MIKE ROGERS, ALABAMA
RANKING MEMBER

One Hundred Sixteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

March 26, 2020

Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Washington, DC 20528

Dear Director Krebs:

The strength and stability of the U.S. health care system has perhaps never been more central to our national and economic security. However, as we work with our partners around the world to contain the rapid spread of COVID-19, I am troubled by recent reports that suggest a corresponding and deeply disturbing rise in malicious cyber activity targeting all parts of the healthcare ecosystem. I would like to understand how the Cybersecurity and Infrastructure Security Agency (CISA), as the lead Federal coordinator for securing critical infrastructure, is working with health care sector partners to prepare for and respond to elevated cyber threats.

Over the past several weeks, we have seen scammers, criminals, and potentially even nation-states carry out cyber campaigns focused on the World Health Organization (WHO), the U.S. Department of Health and Human Services (HHS), and the Centers for Disease Control and Prevention (CDC), to name a few. Some of these cyber operations were likely motivated by profit, while others were designed to impersonate public health authorities, undermine public confidence, gain access to sensitive systems and data, or in some cases, even disrupt delivery of health care services. For instance, last week, a ransomware attack crippled the Brno University Hospital, one of the largest COVID-19 testing centers in the Czech Republic, forcing it to "postpone urgent surgical interventions and re-route new acute patients."[1] Then, over the weekend, we learned that Paris' public hospital system, the Assistance Publique-Hôpitaux de Paris (AP-HP), was hit by a distributed denial of service (DDOS) attack that attempted to overwhelm and disable hospital systems in the midst of an uptick in coronavirus cases.[2]

[1] Catalin Cimpanu, "Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak," *ZDNet* (Mar. 13, 2020), *available at* https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/.

[2] Helene Fouquet, "Paris Hospitals Target of Failed Cyber-Attack, Authority Says," *Bloomberg* (Mar. 23, 2020), *available at* https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says.

Under Federal law, CISA is tasked with coordinating Federal efforts to promote strong cybersecurity within each of the 16 critical infrastructure sectors, including the Healthcare and Public Health (HPH) sector, in coordination with designated Sector Specific Agencies.[3] For the HPH sector, CISA works with HHS, in its capacity as Sector Specific Agency, as well as industry-led coordinating bodies such as the HPH Sector Coordinating Council (HSCC) and the Health Information Sharing and Analysis Center (H-ISAC).

I have no doubt that these critical infrastructure partnerships and programs, though largely voluntary, have had an overall positive impact on cybersecurity within the health sector. In the past month alone, the HSCC released a *Management Checklist for Teleworking Surge During COVID-19 Response*, as well as a set of *Health Industry Cybersecurity Information Sharing Best Practices* to address "real and perceived barriers to information sharing that are often found from laws, regulations, corporate policies or management support, and will help organizations work through these obstacles."[4] Efforts like this are commendable.

At the same time, it is unclear whether they are enough to ensure that the health sector is up to the task of cyber defense in the face of COVID-19. A recent Atlas VPN survey found that the sector remains rife with vulnerabilities, underscoring that "the U.S. is combating COVID-19 while having 83% of their healthcare systems run on outdated software."[5] Last month, the Government Accountability Office (GAO) found that HHS was one of a handful of Sector Specific Agencies that had little to no visibility into whether HPH sector owners and operators were using the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.[6] In describing the Sector Specific Agency construct more broadly, the Cybersecurity Solarium Commission report criticized the "lack of consistency concerning the responsibilities and requirements for these agencies, both within their sectors and in their relations with CISA," which "continues to cause confusion, redundancy, and gaps in resilience efforts."[7]

Our nation is facing an unprecedented crisis, and our health care system is at the center of it. Now more than ever, we need all parts of our health care sector – from hospitals and pharmacies to medical laboratories, surgical operating equipment, and even public health agencies and international authorities – to function as efficiently and effectively as possible.

[3] Sector Specific Agencies are responsible for "providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with [DHS]." Pub. L. 107-296, §2222(5).

[4] Healthcare and Public Health Sector Coordinating Council Critical Infrastructure Security and Resilience Partnership, *Health Industry Cybersecurity Information Sharing Best Practices* (Mar. 2020) *available at* https://healthsectorcouncil.org/info-sharing-guide/.

[5] Atlas VPN Blog, "US is fighting COVID-19 with 83% of systems running on outdated software," (Mar. 2020), *available at* https://atlasvpn.com/blog/us-is-fighting-covid-19-with-83-percent-of-healthcare-systems-running-on-outdated-software/.

[6] GAO-20-299, *Additional Actions Needed to Identify Framework Adoption and Resulting Improvements* (Feb. 2020), *available at* https://www.gao.gov/assets/710/704808.pdf.

[7] The Cyber Solarium Commission was established in the *John S. McCain National Defense Authorization Act for FY 2019*, Pub. L. 115-232, §1652, to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." Its final report was published on March 11, 2020.

Accordingly, pursuant to Rule X(3)(g) of Rule XI of the Rules of the House of Representatives, I respectfully request you provide a written response to the following questions, and whatever supplementary information you deem responsive, by April 10, 2020:

1. How would you characterize the overall cybersecurity posture of the HPH sector, and are there specific areas where CISA would benefit from additional resources or authorities to help ensure health sector partners have robust cybersecurity measures in place to prevent a successful attack, intrusion or disruption?

2. As the world responds to the COVID-19 pandemic, access to healthcare provider networks and patient records will be critical to the prompt delivery of care. How is CISA coordinating with HHS to share actionable cyber threat information and trends to privately- and publicly owned health care sector partners? How is CISA coordinating with HHS to promote good cyber hygiene practices across the healthcare sector to ensure it the sector is prepared to defend against opportunistic cyber-attacks?

3. As indicated above, reports indicate that the 83% of healthcare systems run on outdated software. How is CISA working with HHS to disseminate actionable guidance to mitigate vulnerabilities associated the use of outdated software?

4. What role did CISA play in drafting the HHSC guidance related to managing telework during COVID-19, if any? How has CISA been consulted or otherwise informed the development of any similar past guidance issued by the HSCC or other HPH sector partners?

5. CISA holds itself out as the nation's risk manager, responsible for identifying cross-sector risk and prioritizing activities to manage it. Has CISA engaged in any recent efforts to understand HPH sector-wide and cross-sector risk, particularly in the face of COVID-19? If so, does CISA plan to issue any assessments or reports detailing its findings?

6. Pursuant to the *Cybersecurity Information Sharing Act of 2015* and other Federal statutes, CISA is designated as the primary Federal civilian interface for bi-directional sharing of cyber threat information with the private sector.[8] What channels exist for CISA to either receive information from or share information directly with HPH owners and operators directly, versus through intermediary bodies such as the H-ISAC or HSCC?

7. For cyber threat intelligence that is shared directly with HHS, as the HPH Sector Specific Agency, what protocols exist for ensuring that information is also shared with CISA? How would you characterize the volume and utility of cyber threat information CISA shares and receives with respect to the HPH sector?

Thank you for your attention to this request.

Sincerely,

[8] Pub. L. 114-113, Div. N.

Bennie G Thompson

Bennie G. Thompson
Chairman
Committee on Homeland Security