



October 4, 2018

The Honorable Lamar Alexander
Chairman
Committee on Health, Education,
Labor and Pensions
U.S. Senate

The Honorable Patty Murray
Ranking Member
Committee on Health, Education,
Labor and Pensions
U.S. Senate

The Honorable Greg Walden
Chairman
Committee on Energy and Commerce
U.S. House of Representatives

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
U.S. House of Representatives

Dear Chairman Alexander, Chairman Walden, Ranking Member Frank Pallone, Ranking Member Patty Murray:

Thank you for your letter dated June 5, 2018, regarding efforts by the U.S. Department of Health and Human Services (HHS) to implement the Cybersecurity Act of 2015 (CSA), specifically, the "Cyber Threat Preparedness Report" (CTPR), required by Section 405(b), and the status of Section 405(d), "Aligning Health Care Industry Security Approaches." The Department is committed to improving the security and resiliency of the Healthcare and Public Health (HPH) Sector. The following responses to the Committee's questions reflect the high priority and continued emphasis the Department places on transparency and collaborative public-private partnerships.

HHS drafted the CTPR before the Healthcare Industry Cybersecurity Task Force Report was issued. One of the Task Force recommendations is to "improve information sharing of industry threats, risks, and mitigations." We formed the Healthcare Cybersecurity Command Center (HC3) to enhance HHS' ability to analyze cyber threat information and communicate how emerging threats and vulnerabilities might impact health care. HC3, in coordination with relevant HHS divisions and offices, has produced and disseminated executive and technical summaries on emerging cyber threats that are applicable to a wide range of health care audiences. HC3 developed these products based on information received from a broad range of sources, including private sector organizations, the National Health Information Sharing and Analysis Center (NH-ISAC), and the National Cybersecurity and Communications Integration Center (NCCIC). These products are distributed to healthcare industry partners through the critical infrastructure protection partnership maintained by the Office of the Assistant Secretary for Preparedness and Response (ASPR).

In response to CSA Section 405(d), HHS took several actions, including developing the document, "Cyber Health Practices." This document fosters awareness, promotes best practices,

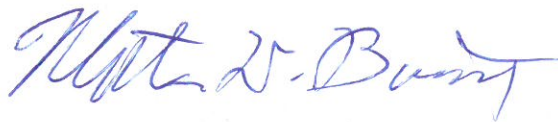
and enhances consistency in mitigating the most pertinent current cybersecurity threats to the sector. To ensure a useful product, HHS convened a development team comprised of a diverse set of healthcare and cybersecurity experts from the public and private sectors. Additionally, the resulting documents have been “pretested” in stakeholder sessions conducted in multiple locations across the United States. The final document was completed on August 31, 2018, is currently in the Departmental clearance process, and HHS has committed to a release date by the end of 2018.

HHS agrees that the CTPR is a living document and will work to incorporate the Committee’s requests. We expect an update by February 2019. These are the planned actions:

1. Update the CTPR with any and all changes and evolutions that have occurred in HHS cybersecurity strategy since the report’s original drafting;
2. Include in the CTPR a detailed explanation of the HC3 that describes roles, responsibilities, the relationship to NCCIC and NH-ISAC, and how the CTPR fits into HHS’ broader cybersecurity capabilities and responsibilities;
3. Add sections to the report explaining how HHS coordinates regulatory authorities among its divisions and offices, and differentiating HHS’ roles as a regulator, as a Sector Specific Agency for the health sector, and in securing its internal environment.

Since the CTPR publication and the release of the Task Force Report, HHS has studied the report’s recommendations and has been working across our Operating Divisions and with Federal partners to continue improving our cybersecurity strategies. HHS was able to take immediate action on some of the recommendations, but others require a longer term approach so that we may align recommendations with existing policies, authorities, and resources. We welcome the opportunity to clarify our cybersecurity strategy, highlight our accomplishments, and discuss the continuing maturation of our cybersecurity strategy as a whole.

Sincerely,



Matthew D. Bassett
Assistant Secretary for Legislation
U.S. Department of Health and Human Services