United States Senate
COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS
WASHINGTON, DC 20510–6300

March 22, 2024

VIA ELECTRONIC TRANSMISSION

The Honorable Xavier Becerra
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C., 20201

Dear Secretary Becerra:

Cybersecurity attacks pose a grave risk to patients. As the Sector Risk Management Agency (SRMA) for the Health and Public Health (HPH) sector, the Department of Health and Human Services (HHS) is the primary coordinating body for cybersecurity incidents. However, recent cyberattacks affecting HHS' internal systems raise questions about its own cybersecurity readiness.

Recent reports indicate that hackers gained access to HHS' own systems and stole approximately $7.5 million in grant awards to be designated to individual awardees, including those administered by the Health Resources and Services Administration (HRSA).[1] This is extremely concerning. HRSA programs serve at-risk populations, including children, pregnant women, and patients in rural populations. The disruption in grant awards caused by this breach has the potential to delay patient care and create financial strain on health care facilities. HHS' lack of transparency and communication regarding this breach, including communication to Congress as required by law, undermines the public trust and suggests that the Federal government is not prepared to protect patients against cybersecurity attacks.

Americans entrust HHS to safeguard taxpayer dollars from cyberattacks. An unauthorized breach of this nature requires transparency from HHS about the facts at issue, and leadership from HHS to take the necessary steps to ensure that it does not happen again. As such, in an effort to better understand the facts surrounding this incident and HHS' remedial efforts, I ask that you answer the following questions, on a question-by-question basis, by **April 5, 2024:**

[1] Riley Griffin, *Hackers Stole $7.5 Million in Grant Money from US Health Department*, BLOOMBERG (Jan. 18, 2024), https://www.bloomberg.com/news/articles/2024-01-18/us-health-department-cyber-attack-led-to-millions-in-grant-money-being-stolen.

1. When did HHS become aware of the unauthorized access to the Payment Management Services (PMS) system that processes grant awards?

2. On what date were unauthorized entities able to access the PMS system?

3. How many grantees were affected by the breach? Please quantify the amount of grant funds stolen from the PMS system.

4. When did HHS notify other federal agencies of the breach, including the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), the Executive Office of the President, and the 15 other cabinet and non-cabinet agencies who also use the PMS system?

5. What safeguards did HHS have in place prior to the breach to monitor suspicious activity regarding the PMS system?

6. Has the breach of the PMS system delayed payment of any grant awards? If so, how has HHS communicated these delays to awardees?

7. What steps has HHS taken to recover any and all funds stolen as a result of the breach?

8. What remedial actions has HHS taken to date to improve any vulnerabilities exploited through this breach?

9. The Federal Information Security Modernization Act (FISMA) requires federal agencies to disclose breaches of internal systems to Congress within seven days of determining "it has a reasonable basis to conclude that a major incident, including a breach constituting a major incident, has occurred."[2] HHS, however, has yet to provide the required FISMA notice to Congress.

    a. What is HHS' justification for failing to provide this notice?
    b. If HHS intends to provide a notice for Congress, when will it do so?

10. Please provide the name and title for the employee at HHS responsible for:

    a. Monitoring the PMS system?
    b. Reporting any breaches to the Department?
    c. Coordinating the cyber response within the Department?
    d. Coordinating the cyber response with other federal entities?
    e. Providing the required FISMA notification to Congress?

---

[2] *Memorandum M-23-03*, OFFICE OF MANAGEMENT AND BUDGET (Dec. 2, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/12/M-23-03-FY23-FISMA-Guidance-2.pdf.

11. Does HHS currently have an internal incident response plan in place when responding to cyber incidents? If so, when was it last updated? If not, please provide a justification for the lack of plan.

Sincerely,

Bill Cassidy, M.D.

Bill Cassidy, M.D.
Ranking Member
U.S. Senate Committee on Health,
Education, Labor, and Pensions