June 30, 2016

The Honorable Joseph R. Pitts
Chairman, Subcommittee on Health
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Pitts,

Thank you for the opportunity to appear before the before the Subcommittee on Health on May 25, 2016, to testify at the hearing entitled “Examining Cybersecurity Responsibilities at HHS.” CHIME and its members take very seriously their responsibility to protect their networks and patient data from cyber criminals. The hearing focused a critical and timely issue for our members. Attached please find my written responses to the questions for the record.

Sincerely,

Marc Probst
Vice President and Chief Information Officer, Intermountain Healthcare
Board of Trustees Chairman, College of Healthcare Information Management Executives

cc: The Honorable Gene Green, Ranking Member, Subcommittee on Health

Attachment

The Honorable Joseph R. Pitts

**Throughout the hearing, members of the panel either made or agreed with the assertion that H.R. 5068 will not work in a vacuum; HHS must also have clear, effective, and enforced policies, procedures, and processes for ensuring that cybersecurity is a priority throughout the Department.**

1. **Please describe the policies, procedures, and processes that you believe HHS currently has in place for ensuring that cybersecurity is a priority throughout the Department.**

Just as healthcare institutions must coordinate efforts to thwart cyber threats, it is vital that the Department of Health and Human Services (HHS) have a coordinated plan to address threats to the data and systems used and housed by the department. The Cybersecurity Act of 2015 calls on HHS to present to Congress within a year a report that identifies the individual who will be responsible for coordinating and leading efforts to combat cybersecurity threats. HHS must also present a plan detailing how each operational division will address cybersecurity threats in the healthcare industry, and a delineation of how personnel within each division will communicate with each other regarding efforts to address such threats.

The forthcoming coordination plan, in conjunction with the output of the Health Care Industry Cybersecurity Task Force, will be an important mechanism to evaluate current practices employed within HHS and help identify any weakness that must be addressed. Understanding these weaknesses will benefit both HHS and the industry.

In addition to the directive from the Cybersecurity Act of 2015, HHS launched an enterprise-wide information security and privacy program in fiscal year 2003 to help protect against potential information technology (IT) threats and vulnerabilities. The program ensures compliance with federal mandates and legislation, including the Federal Information Security Management Act and the President’s Management Agenda. The HHS Cybersecurity Program plays an important role in protecting HHS' ability to provide mission-critical operations. In addition, the HHS Cybersecurity Program is the cornerstone of the HHS IT Strategic Plan, and an enabler for e-government success.

2. **Are there policies, procedures, and processes that you believe HHS should adopt in order to be more effective with regards to cybersecurity?**

No industry can enable perfect security; rather, organizations must enumerate and manage their risks. At a healthcare organization, the IT security team is challenged with understanding every possible avenue of attack by which a hacker might gain access to the network, including malicious malware or intrusion via a weak link in devices or part of the facility’s infrastructure that receive routine electronic updates. A hacker only needs to find and exploit one weakness to penetrate a network. That’s as true for HHS and its operating divisions as it is for a hospital.

In many cases, that one weakness is preying upon the behaviors of individuals through social engineering. As many studies have shown, and as many organizations that conduct penetration tests and other social engineering assessments will attest, it is impossible to prevent every human being in an organization from falling prey to such an attack. Coordination and a clear delineation of responsibilities across an organization are key tenets of an effective cybersecurity strategy, whether it is a healthcare delivery organization or the Department of Health and Human Services. Clear and consistent communication, reinforced by vigilant training programs, will allow a strategy to flourish.

We are hesitant to suggest the immediate adoption of particular policies until HHS has completed its report to Congress.

3. **Are there policies, procedures, or processes that you believe that HHS should consider reforming or removing in order to be more effective with regards to cybersecurity?**

HHS' coordination plan, which is expected to be delivered to Congress in December, should show areas for improvement in HHS' cyber protocols and procedures. That said, security must be an organizational priority for true change to take hold. Even before the coordination plan is delivered to Congress, HHS could embark on a comprehensive training program that creates a set of expectations and holds staff accountable. For instance, many healthcare organizations will routinely conduct phishing exercises to assess employee behavior and detect trouble spots.

**Throughout the hearing, members of the panel emphasized that, in addition to its organizational structure, it is critically important the roles and responsibilities for officials within HHS in regards to cybersecurity are clear and effective.**

4. **Please describe the responsibilities and authorities that you believe the following HHS officials should have with regards to cybersecurity:**

- **The Secretary of Health;**
- **The HHS CIO;**
- **The HHS CISO**
- **Any other officials (such as the General Counsel, CFO, etc.).**

Given the breadth and depth of cyber threats, it's paramount that all facets of the department, from the information technology department to researchers at the National Institutes of Health (NIH) to senior leadership and everyone in between, coordinate efforts to improve HHS' cyber hygiene.

- **The Secretary of Health**

Similar to a hospital and health system CEO or in some cases, members of a health system's board of directors, the secretary has a responsibility to understand, at a high level, the risks and vulnerabilities the department faces. The secretary must use his/her bully pulpit to make cybersecurity an organization priority and ensure that risk management and risk mitigation is part of an overall operational plan.

The secretary should know who within the department is responsible for the execution and implementation of the cybersecurity plan. Given that cybersecurity should not be considered solely an information technology issue, it's imperative that the secretary have regularly scheduled meetings with the chief information officer (CIO) and/or other members of the department's cybersecurity team, which should include: Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Chief Security Officer (CSO).

- **The HHS CIO**

As in healthcare delivery organizations, the CIO should manage various pieces of the department's information technology infrastructure, with responsibility over the myriad of IT and computer systems that support the department's enterprise-wide goals, including information security. Currently, the CIO advises the secretary and the Assistant Secretary for Resources and Technology (ASRT) on matters pertaining to the use of information and related technologies.

Within HHS, the Office of the Chief Information Officer should, among other responsibilities, provide assistance and guidance on the use of technology-supported business processes; investment analysis for information technology; strategic development and application of information systems and infrastructure; and, establish and execute policies to provide improved management of information resources and technology within the department.

- **The HHS CISO**

As I mentioned in my testimony, the reporting structure for CISOs varies across healthcare organizations. At Intermountain Healthcare, the CISO reports directly to me, the CIO. More important that the reporting structure is ensuring coordination and continuity of an organizatino's cybersecurity plan. Similar to the private sector, the HHS' CISO should be focused on developing and overseeing the implementation of the *technical strategy to achieve the department's security posture,* as well as managing the department's information security team. Working across information systems operations ensures that the technical components required for cybersecurity are in place and managed.

**In the hearing, the panel discussed the fact that, as currently drafted, H.R. 5068 makes the newly elevated CISO a presidential appointment. Concerns were raised about that, stating that it might overly politicize the position.**

5. **Would the position be more effective if it wasn't a presidential appointment?**

As a former member of the Health IT Policy Committee, a federal advisory committee created under Health Information Technology for Economic and Clinical Health Act (HITECH), I witnessed firsthand how important initiatives for improving care delivery can get bogged down in politics and bureaucracy resulting from political appointments. What's central to this conversation is the value of meaningful coordination, avoiding any unintended consequences of complex reporting structure. For instance, elevating the CISO to a presidential appointment could create tensions with other with other positions that, at least on the department's organization chart, have equal responsibilities, but are not appointed. Such a circumstance may impede the coordination and flow of information necessary to thwart cyber threats due to the nature by which an individual was selected for their position.

It is vital to fully evaluate the potential negative consequences that could result from making the HHS CISO a presidential appointment. We've seen instances where politicizing a role can hamper an agency's ability to affect change. For instance, confirmation hearings can be delayed for a variety of reasons, leading to a void in leadership. The CISO, as with the CIO, demand significant technical expertise. A presidential appointment could unnecessarily imperil the chances that qualified, rather than connected, candidates fill the office.

CHIME recommends that the CISO within the Department of Health and Human Services not be a presidentially-appointed position.