U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

May 23, 2016

TO: Members, Subcommittee on Health

FROM: Committee Majority Staff

RE: Hearing on “Examining Cybersecurity Responsibilities at HHS”

On Wednesday, May 25, 2016, at 10:00 a.m. in 2123 Rayburn House Office Building, the Subcommittee on Health will hold a hearing entitled “Examining Cybersecurity Responsibilities at HHS.” This hearing will examine the organizational alignment of the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) at the Department of Health and Human Services (HHS). An August 2015 Committee report concluded that the current organizational structure of these positions was at least partially responsible for information security incidents throughout the Department. The hearing will also examine H.R. 5068, HHS Data Protection Act, which implements a key recommendation of the August 2015 report that would elevate and empower the HHS CISO.

I. WITNESSES

- Joshua Corman, Director, Cyber Statecraft Initiative, Atlantic Council;
- Mac McMillan, Chief Executive Officer, CynergisTek, Inc.;
- Samantha Burch, Senior Director, Congressional Affairs, Healthcare Information and Management Systems Society North America; and,
- Marc Probst, Vice President and Chief Information Officer, Intermountain Healthcare, on behalf of the College of Healthcare Information Management Executives.

II. BACKGROUND

In August 2015, Committee staff released the results of a year-long investigation into the state of information security at HHS.[1] At its inception, the investigation focused on an October 2013 breach of the Food and Drug Administration (FDA), but expanded to include information security incidents at other HHS operating divisions that came to light in the course of the investigation. In total, Committee staff identified incidents at five operating divisions that occurred over a span of three years. These incidents, coupled with several Office of Inspector

[1] STAFF OF H. COMM. ON ENERGY AND COMMERCE, 114th Cong., REPORT ON THE DEPT. OF HEALTH AND HUMAN SERVICES INFORMATION SECURITY (2015).

General and Government Accountability Office reports reviewed during the investigation revealed pervasive and persistent deficiencies across HHS and its operating divisions' information security programs.

Ultimately, the report concluded that many of these deficiencies shared a primary root cause – the subordination of information security concerns to information operations concerns. In information security the need to maintain progress or to keep systems operational is in constant tension with the need to make progress safely, or to operate systems in a secure way. The Committee's investigation found that at HHS, this tension often favors information operations, resulting in information security being treated as a "release valve" when operational pressures mount.

Evidence uncovered during the Committee's investigation suggests that this subordination of security concerns to operational concerns stems from the organizational relationship between the CIO and CISO at both HHS headquarters and throughout its operating divisions. At present, the CIO, whose primary responsibility is the deployment, operation, and maintenance of information technology systems, is the direct supervisor of the CISO, whose primary responsibility is the security of those information technology systems. Due to this organizational hierarchy, information security is automatically subordinated to information operations. Specific incidents at FDA, the Centers for Medicare and Medicaid Services, and the Office of Civil Rights examined in the report demonstrate the negative consequences of this subordinate relationship,[2] and Committee staff further concluded that additional weaknesses in HHS and its operating divisions' information security programs likely also stem from this same root cause.

To address this issue and ensure that information security is appropriately prioritized at HHS and its operating divisions, the report recommended that HHS separate information security from information operations by relocating the HHS CISO out of the HHS CIO's chain of command. In doing so, the report argued that HHS would eliminate the inherent subordination of security to operations created by the current organizational hierarchy, and remove the ability for information security to be used as a "release valve" for operational pressures.

This reorganization would follow a growing trend in the private sector and at least one other federal agency, where experts have acknowledged the drawbacks of the traditional CIO-CISO reporting structure. For example:

- A 2014 study from PricewaterhouseCoopers found that:
  - "[O]rganizations in which the CISO reported to the CIO experienced 14% more downtime due to cyber security incidents than those organizations in which the CISO reported to the CEO" and,[3]

[2] *Id* at 16-17
[3] PRICEWATERHOUSECOOPERS, THE GLOBAL STATE OF INFORMATION SECURITY SURVEY 2014 (2014).

  - "[H]aving the CISO report to almost any position in senior management *other* than the CIO (Board of Directors, CFO, etc.), reduced financial losses from cyber incidents."[4]

- In the 2016 update of the PricewaterhouseCoopers report, the authors argue that "[w]hile there are some exceptions, we believe that CISOs and [Chief Security Officers] should be independent of CIOs to better allow for internal checks and balances, as well as to escalate security issues to corporate leadership and the Board."[5]

- The Defense Threat Reduction Agency (DTRA) of the Department of Defense abandoned the traditional CIO-CISO structure in favor of one wherein the Director of Security – the functional equivalent of the CISO – is a peer to the CIO. Mac McMillan, the former Director of Security for DTRA, explains that at DTRA, "the CIO cannot deploy any systems on his own. All information systems have to be signed off on by the director of security. It's a matter of checks and balances."[6]

III. LEGISLATION UNDER CONSIDERATION

On April 26, 2016, Rep. Billy Long (R-MO) and Rep. Doris Matsui (D-CA) introduced the bipartisan H.R. 5068, HHS Data Protection Act, to enact this organizational reform at HHS. H.R. 5068 elevates and empowers the current HHS CISO with the creation of a new office, the Office of the Chief Information Security Officer, which will operate as an organizational peer to the HHS CIO. Additionally, H.R. 5068 designates the HHS CISO as the primary authority for information security at HHS, thereby removing information security responsibilities from the HHS CIO and consolidating those responsibilities within a single office at the Department.

IV. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Jessica Wilkerson or J.P. Paluskiewicz with the Committee staff at (202) 225-2927.

[4] *Id.*
[5] PRICEWATERHOUSECOOPERS, THE GLOBAL STATE OF INFORMATION SECURITY SURVEY 2016 19 (2016).
[6] Marianne Kolbasuk McGee, *Proposed Legislation Aims to Elevate HHS CISO Role*, HEALTHCARE INFO SECURITY, May 3, 2016, http://www.healthcareinfosecurity.com/proposed-legislation-aims-to-elevate-hhs-ciso-role-a-9080.