

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

May 23, 2016

To: Subcommittee on Health Democratic Members and Staff
Fr: Committee on Energy and Commerce Democratic Staff
Re: Hearing on “Examining Cybersecurity Responsibilities at HHS”

On Wednesday, May 25th, at 10:00 a.m., in Room 2123 of the Rayburn House Office Building, the Subcommittee on Health will hold a hearing titled “Examining Cybersecurity Responsibilities at HHS.”

I. BACKGROUND

Cybersecurity represents a growing challenge, both for the private sector and the federal government. Since FY 2006, the number of information security incidents affecting systems supporting the federal government has steadily increased each year: rising from 5,503 in FY 2006 to 67,168 in FY 2014, an increase of 1,121 percent.¹ The number of reported security incidents involving personally identifiable information (PII) at federal agencies has more than doubled in recent years—from 10,481 incidents in FY 2009 to 27,624 incidents in FY 2014.² One example of a recent high-profile breach within the federal government is the 2014 breach of the Office of Personnel Management and two of its contractors, which resulted in the compromise of the PII of as many as 21.5 million Americans.³

The Office of the Chief Information Officer within the Department of Health and Human Services (HHS) currently leads the development and implementation of information technology

¹ Government Accountability Office (GAO), *Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies* (June 24, 2015) (GAO-15-725T).

² *Id.*

³ Office of Personnel Management, *Cybersecurity Resource Center* (online at www.opm.gov/cybersecurity/cybersecurity-incidents/).

(IT) infrastructure across the agency.⁴ At present, the office is tasked with a variety of responsibilities, including: e-government initiatives, IT operations management, IT investment analysis, IT security and privacy, performance measurement, policy development, strategic information system and infrastructure development and application, and technology supported business process reengineering.⁵

II. FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

The principal law concerning the federal government’s information security program is the 2002 Federal Information Security Management Act (FISMA). This law requires federal agencies to provide information security protections for agency information systems.⁶ Under FISMA, federal agencies are required to provide protections for agency information systems and information collected or maintained by agencies “commensurate with the risk and magnitude of the harm” that could result from unauthorized access or disruption.⁷

Under FISMA, each agency must designate an information security officer to implement these monitoring and protection responsibilities.⁸ FISMA also assigns specific responsibilities for information security to the head of each agency, as well as to each agency’s Chief Information Officer.⁹ Each agency is required to implement an information security program that includes periodic assessments of the risk to the agency’s information and information systems, ensures that information security is addressed throughout the life cycle of the information system, and ensures compliance with policies issued by the Office of Management and Budget (OMB) and standards issued by the National Institute of Standards and Technology (NIST).¹⁰

According to the U.S. Government Accountability Office (GAO), IT security management remains a major challenge for all federal agencies. Of the 24 federal agencies covered by FISMA, nearly all had weaknesses in the five major security control categories in fiscal year 2012.¹¹

III. H.R. 5068, HHS DATA PROTECTION ACT

⁴ U.S. Department of Health and Human Services (HHS), *About the OCIO: What We Do* (online at <http://www.hhs.gov/ocio/about/whatwedo/what.html>).

⁵ *Id.*

⁶ Federal Information Security Management Act of 2002; 44 U.S.C. § 3543.

⁷ 44 U.S.C. § 3544.

⁸ *Id.*

⁹ *Id.*

¹⁰ Congressional Research Service, *Cyber Security: FISMA Reform* (Dec. 15, 2014).

¹¹ GAO, *Information Security: Federal Agencies Need to Enhance Responses to Data Breaches* (Apr. 2, 2014) (GAO-14-487T).

H.R. 5068, the HHS Data Protection Act, as proposed by Representatives Billy Long (R-MO) and Doris Matsui (D-CA), would elevate the position of the HHS Chief Information Security Officer (CISO) to the same organizational level as the Chief Information Officer (CIO).¹² The bill is based on an investigation performed by the Energy and Commerce Committee Majority Staff (see below). Under the new arrangement, both the CISO and CIO would report at the same level to the Assistant Secretary for Administration. Presently, the CISO reports to the CIO, as is statutorily required under FISMA. The CISO would be appointed by the President.

The proposal states that the CISO shall maintain primary responsibility for the information security (including cybersecurity) programs of the HHS. The bill specifies that it would transfer all functions, personnel, assets, and liabilities of the current CISO to the new, elevated office.

Finally, H.R. 5068 requires that no later than one year after the IT security program's enactment of the bill, the Secretary shall submit a report to Congress describing implementation of the change. Specifically, it requires a detailing of the plan of the CISO to oversee and coordinate in the Department as well as steps being taken within each operating division's implementation plan.

IV. MAJORITY STAFF INVESTIGATION

In August 2015, the majority issued a staff report entitled, "Information Security at the Department of Health and Human Services."¹³ The report details several information security breaches to the Department's information systems, including a breach at the Food and Drug Administration's (FDA) Center for Biologics Evaluation and Research (CBER) in October 2013, as well as several other "relatively minor" security incidents involving the National Institutes of Health, the Health Resources and Services Administration, the Substance Abuse and Mental Health Services Administration, the Indian Health Service and the Centers for Medicare and Medicaid Services.¹⁴

The report concludes that information security is not accorded adequate priority at HHS due partly to the organizational hierarchy of officials and offices, as configured under the FISMA framework. The current organizational structure that exists at HHS and its operating divisions, as well as at most federal agencies, involves a Chief Information Security Officer (CISO) that reports to a Chief Information Officer (CIO). The report recommends the following organizational changes:

¹² H.R. 5068.

¹³ House Committee on Energy and Commerce, Majority Staff, *Information Security at the Department of Health and Human Services* (Aug. 6, 2015) (online at <https://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/114/Analysis/20150806HHSinformationsecurityreport.pdf>).

¹⁴ *Id.*

- CISOs should be designated as the primary authority responsible for information security at HHS and its operating divisions, and all information security responsibilities currently assigned to the CIO should be officially transferred to the CISO.
- The HHS Office of the CISO, including all functions, personnel, assets, and liabilities, should be removed from the Office of the CIO and relocated to the Office of the General Counsel.
- The Office of the CISO for each HHS operating division, including all functions, personnel, assets, and liabilities, should be removed from the Office of the CIO and relocated to the operating division's Office of the Chief Counsel.¹⁵

V. RELATED LEGISLATION

In December 2015, H.R. 2029, the Consolidated Appropriations Act, was signed into law. This bill included related cybersecurity legislation, specifically the Cybersecurity Information Sharing Act of 2015 (CISA).¹⁶ CISA included provisions aimed at improving cybersecurity in the health care industry. First, it required a report from the Secretary of HHS that would include a clear designation of an official within HHS who is responsible for leading and coordinating efforts to combat cybersecurity threats within HHS and the health care industry. The report will also outline a plan for each relevant operating division and subdivision of HHS outlining specific approaches for cybersecurity threats as well as personnel responsibilities.

In addition to the agency report, the bill also created a Health Care Industry Cybersecurity Task Force. Members of this task force were recently appointed, and are expected to deliver the finalized Task Force report by March 2017.¹⁷ The broad goal of the group is to enhance the federal government's cybersecurity, including both defensive and offensive capabilities.

The required content of the Task Force report was outlined in CISA. It specifies that the report include an evaluation of how other industries have addressed cybersecurity threats, review challenges facing network security and establish an implementation plan so that the federal government and industry stakeholders may share actionable cyber threat indicators and defensive measures in real time. Finally, it requires the report deliver its findings and recommendations to Congress.

¹⁵ *Id.*

¹⁶ H.R. 2029.

¹⁷ HHS, *Health Care Industry Cybersecurity Task Force* (Mar. 17, 2016) (online at <http://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx>).

VI. WITNESSES

Josh Corman

Director
Cyber Statecraft Initiative
Atlantic Council

Samantha Burch

Senior Director
Congressional Affairs
Healthcare Information and Management Systems Society

Mac McMillan

Chief Executive Officer
CynergisTek, Inc.

Marc Probst

Vice President & Chief Information Officer
Intermountain Healthcare
On behalf of College of Healthcare Information Management Executives (CHIME)