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

June 6, 2017

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing on "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity"

I. INTRODUCTION

The Subcommittee on Oversight and Investigations will hold a hearing on Thursday, June 8, 2017, at 10:15 a.m. in 2322 Rayburn House Office Building. The hearing is entitled "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity."

This hearing will provide an opportunity for officials from the Department of Health and Human Services (HHS) to educate Members of the Subcommittee on the Department's role regarding cybersecurity in the health care sector. In particular, the hearing will focus on findings from two reports that Congress required HHS to produce under the Cybersecurity Act of 2015,[*] examining both HHS' internal cybersecurity processes and industry recommendations for improving cybersecurity across the sector. Finally, this hearing will use the recent global outbreak of "WannaCry" ransomware, and HHS' subsequent response, as a case study for the effectiveness and applicability of the findings from the reports.

II. WITNESSES

- Steve Curren, Director for the Division of Resilience, Office of Emergency Management, Office of the Assistant Secretary for Preparedness and Response, Department of Health and Human Services;
- Leo Scanlon, Deputy Chief Information Security Officer, Department of Health and Human Services;[1] and,
- Emery Csulak, Chief Information Security Officer and Senior Privacy Official, Centers for Medicare and Medicaid Services; Co-Chair, Health Care Industry Cybersecurity Task Force.

III. BACKGROUND

[*] A previous version of this memorandum cited the Cybersecurity Information Sharing Act of 2015 (CISA), which was included within the Cybersecurity Act of 2015 (CSA). References to CISA have been changed to CSA throughout this memorandum.

[1] Leo Scanlon is also the HHS designee for cybersecurity required under Section 405(b)(2)(A) of the Cybersecurity Act of 2015.

Over the past several years, the health care sector has become increasingly digitized and integrated with information technology. These technologies have created significant benefits, including the improved efficacy of care, increased patient engagement, and faster discovery of treatments and cures. However, with these benefits comes an increased risk of cybersecurity threats. As the health care sector's dependence upon and integration with information technology has grown, so too have cybersecurity incidents within the sector such as malware infections,[2] large-scale thefts of medical data,[3] and the discovery of critical vulnerabilities in medical devices.[4,5,6]

In recognition of this growing threat, Congress included language in the Cybersecurity Act of 2015 (CSA) that required the Department of Health and Human Services to produce two reports examining cybersecurity within the health care sector, one focused internally within the Department itself, and the other externally within the health care sector.[7]

A. The HHS Cyber Threat Preparedness Report

The first review, required under section 405(b) of CSA, instructed HHS to submit to Congress a report on the Department's preparedness to respond to cybersecurity threats within the health care sector.[8] Section 405(b) further required two primary findings: a statement identifying the official to be responsible for leading and coordinating Department cybersecurity efforts, and a plan from each relevant operating division detailing how that operating division intended to address cybersecurity threats within their jurisdiction. In response, the report included the following findings, among others:

- The Department identified the Deputy Secretary, or their designee, as the official responsible for leading and coordinating Department cybersecurity efforts;

- The Office of the Assistant for Preparedness and Response (ASPR) has primary responsibility for cybersecurity efforts within the Department;

---

[2] Naomi Lachance, *Malware Attacks on Hospitals Put Patients At Risk*, NPR, Apr. 1, 2016, http://www.npr.org/sections/alltechconsidered/2016/04/01/472693703/malware-attacks-on-hospitals-put-patients-at-risk.
[3] Dan Munro, *Data Breaches in Healthcare Totaled Over 112 Million Records in 2015*, FORBES, Dec. 31, 2015, https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#56e1a0c27b07.
[4] *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*, FDA, Jul. 31, 2015, https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm456815.htm.
[5] *Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication*, FDA, Jan. 9, 2017, https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm.
[6] *Johnson & Johnson Warns Patients of an Insulin Pump Cyber Bug*, REUTERS, Oct. 4, 2016, http://fortune.com/2016/10/04/johnson-johnson-insulin-pump-cyber-bug/.
[7] Consolidated Appropriations Act, 2016, 6 U.S.C. § 1533 (2017).
[8] *Id.*

- Eleven components within the Department contribute to health care sector cybersecurity threat preparedness;[9] and,

- The Department leverages an internal working group that includes relevant officials from across these different offices and operating divisions to coordinate cybersecurity efforts.

In briefings following the release of the internal HHS Cyber Threat Preparedness report, officials from the Department informed the Committee that cybersecurity roles, responsibilities, and efforts continue to evolve. Most importantly, the Department is in the process of standing up the Health Cybersecurity and Communications Integration Center (HCCIC).[10] The HCCIC is intended to serve as a nexus for information, collaboration, and analysis regarding cybersecurity threats in the health care sector. It is likely to have a significant impact on the processes and procedures the Department uses to address cybersecurity threats and engage with industry. As a result, some findings in the HHS Cyber Threat Preparedness report may soon be outdated.

B. The Health Care Industry Cybersecurity Task Force

The second review, required under section 405(c) of CSA, instructed the Department to convene a task force consisting of stakeholders from HHS, the Department of Homeland Security, the National Institute of Standards and Technology, and the health care sector, as well as cybersecurity experts.[11] The task force report includes six imperatives, broken down into 27 specific recommendations, including the following:

- Industry should leverage information sharing programs to better manage cybersecurity risks and vulnerabilities;

- Industry must adopt coordinated vulnerability disclosure policies and procedures;

- Industry must develop "bills of materials" for their products that identify their components and any known risks associated with those components;

- Industry should explore ways to secure and replace legacy systems; and,

- Industry should explore ways to better enable and ensure timely patching of information technologies within the health care environment.

---

[9] The relevant components are: the Office of the Secretary; the Office of the Assistant Secretary for Administration; ASPR; the Office of Civil Rights; the Office of the Inspector General; the Office of the National Coordinator for Health Information Technology; the Centers for Disease Control and Prevention; the Centers for Medicare and Medicaid Services; the Food and Drug Administration; the Indian Health Service; and the National Institutes of Health.

[10] Nicole Ogrysko, *HHS to stand up its own version of the NCCIC for health*, FEDERAL NEWS RADIO, Apr. 20, 2017, https://federalnewsradio.com/health-it/2017/04/hhs-to-stand-up-its-own-version-of-the-nccic-for-health/.

[11] *See supra* note 7.

These recommendations reflect the input and consensus of officials from relevant federal government agencies, cybersecurity experts, and representatives of health care organizations themselves. As such, it is expected that the Health Care Industry Cybersecurity Task Force report will form a primary basis for future work in better addressing health care cybersecurity issues.

C. Case Study: The "WannaCry" Ransomware Outbreak

On March 12, 2017, an outbreak of the type of file-encrypting malware known as "ransomware" spread quickly across the globe, infecting hundreds of thousands of devices in dozens of countries in a matter of hours.[12] Dubbed "WannaCry," this strain of ransomware leveraged a powerful and widespread flaw in a popular computer operating system to spread quickly from device to device. Once infected with WannaCry ransomware, devices became impossible to use until either a ransom had been paid to the ransomware authors through the virtual currency Bitcoin, or the device was restored from a backup.[13]

While nearly all industries and sectors were affected by the WannaCry outbreak, particular attention was focused on the health care sector due to the infection of 40 National Health System (NHS) hospitals in the United Kingdom.[14] These infections forced the hospitals to drastically reduce services, cancel certain operations, and in some cases, turn away all but emergency patients.[15,16] Following news of the NHS infections, concerns were immediately raised about the susceptibility of United States health care organizations to the outbreak. However, efforts by cybersecurity companies, independent experts, and private-sector organizations eventually led to the containment of the ransomware before it could infect more than a small number of devices in the United States.[17,18]

Though the effect on health care organizations in the United States was ultimately minimal, the sector was nonetheless extremely susceptible to the ransomware outbreak, and remains so today.[19,20] Many experts in both the cybersecurity and health care industries acknowledge that, had the ransomware not been contained when it was, the United States would

---

[12] Lily Hay Newman, *The Ransomware Meltdown Experts Warned About is Here*, WIRED, Mar. 12, 2017, https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.
[13] *What you need to know about the WannaCry Ransomware*, SYMANTEC, May 12, 2017, https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware.
[14] João Medeiros, *WannaCry laid bare the NHS' outdated IT network – and it's still causing problems*, WIRED UK, May 24, 2017, http://www.wired.co.uk/article/nhs-cyberattack-it-ransomware.
[15] *NHS England – Statement on reported NHS cyber attack*, NHS ENGLAND, May 12, 2017, https://www.england.nhs.uk/2017/05/statement-on-reported-nhs-cyber-attack/.
[16] NHS Lanarkshire (@NHSLanarkshire), Twitter (May 12, 2017, 11:22 AM), https://twitter.com/NHSLanarkshire/status/863097050090622977.
[17] Elisabeth Weise & Mike Snider, *How U.S. dodged a bullet in Friday's massive global ransomware attack*, USA TODAY, May 15, 2017, https://www.usatoday.com/story/tech/news/2017/05/15/ransomeware-attack-wannacry-malware/101710900/.
[18] Lily Hay Newman, *How An Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack*, WIRED, May 13, 2017, https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/.
[19] *Id.*
[20] Beau Woods, *The NHS got lucky – for now. Cyber attacks will only get worse*, THE GUARDIAN, May 15, 2017, https://www.theguardian.com/commentisfree/2017/may/15/nhs-cyber-attacks-ransomware-crisis.

likely have experienced a severe outbreak that could have led to significant impacts on the ability of the health care sector to function.[21]

As the federal government agency responsible for regulating the health care sector, the Department played a critical role in responding to the WannaCry ransomware outbreak. The Department reported that, beginning the day of the outbreak and peaking over the following several days, it took a central role in coordinating government resources and expertise, compiling and distributing relevant information, and generally serving as a hub for both public- and private-sector response efforts. As outlined in the internal HHS Cyber Threat Preparedness Report, the HHS Deputy Secretary's designee for cybersecurity and an official from ASPR took primary lead, with other relevant Department operating divisions providing support as necessary.

Initial feedback from both the Department and from the health care sector has generally concluded that the Department's response, and therefore its cyber threat preparedness strategy as envisioned in its report, was effective. In addition, many of the factors identified as responsible for the susceptibility of the United States health care sector to the WannaCry ransomware outbreak are discussed in the Health Care Industry Cybersecurity Task Force report, along with recommendations regarding how to better address those factors.[22] However, given the continued evolution of cybersecurity roles and responsibilities at the Department, and the recent release of the Task Force report, significant work remains to be done to ensure that both the Department and the health care sector are fully prepared to respond to cyber threats.

IV. ISSUES

The following issues may be addressed at the hearing:

- The effectiveness of the Department's strategy for maintaining cyber threat preparedness;
- How the continued evolution of cybersecurity roles and responsibilities, including the deployment of the HCCIC, will affect the Department's cyber threat preparedness strategy;
- How the Department plans to leverage and incorporate the findings from the Health Care Industry Cybersecurity Task Force report;
- How the Department intends to support industry as it explores ways to leverage and incorporate the findings from the Health Care Industry Cybersecurity Task Force report; and

[21] *See supra* notes 12, 17, 18, and 20.
[22] Experts from both the cybersecurity and health care industries have cited the presence of legacy systems in health care networks and the absence of critical cybersecurity patches, among others, as primary factors of the susceptibility of health care organizations to the WannaCry ransomware outbreak. *See supra* notes 12, 17, 18, and 20.

- The "lessons learned" that the Department has taken from the WannaCry ransomware outbreak, and how those lessons will inform the Department's cybersecurity efforts.

V. STAFF CONTACTS

Please contact Jessica Wilkerson or John Ohly of the Committee staff at (202) 225-2927 with any questions.