June 23, 2017

Mr. Emery Csulak
Chief Information Security Officer and Senior Privacy Official
Centers for Medicare and Medicaid Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Mr. Csulak:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Thursday, June 8, 2017, to testify at the hearing entitled "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Friday, July 7, 2017. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Ali.Fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Attachment—Additional Questions for the Record

The Honorable Tim Murphy

1. At the hearing, Ms. Walters asked Mr. Scanlon whether the Department of Homeland Security (DHS) was aware of or involved in HHS's decision to establish the HCCIC. In response, Mr. Scanlon stated there were "extensive discussions" with DHS. He added, "In fact, it was -- it was people in the Department of Homeland Security who suggested that we move and think in this direction."

    a. What individuals at the Department of Homeland security suggested that HHS should consider establishing an HCCIC? When did this occur?

    b. How did this come up in conversation with DHS? Was this concept initially proposed by DHS or did HHS raise the idea with DHS and they encouraged the Department to pursue this course?

    c. What is HHS's understanding of why DHS suggested the Department move in this direction?

2. This hearing was the second that this subcommittee has had focused on healthcare cybersecurity. The first involved witnesses from the private sector side of the healthcare industry. In response to Member questions, witnesses at that first hearing explained that one of the challenges facing the sector regarding health care cybersecurity is confusion about which offices and officials are responsible for cybersecurity at the Department of Health and Human Services (HHS).

    a. Now that HHS has completed an internal review of its cybersecurity responsibilities, how does HHS intend to communicate these findings to the sector?

    b. Will HHS publicly announce Mr. Scanlon's appointment as the cybersecurity designee, and will this announcement include an explanation of his duties and responsibilities?

    c. Will HHS publicly clarify the role that each relevant office or component fills with regards to cybersecurity?

The Honorable Michael Burgess

1. As healthcare is looking for greater interoperability and the ability to seamlessly share data in a secure manner, what can be done to ensure that the data remains accurate and secure?

2. The Report on Improving Cybersecurity in the Health Care Industry, produced by the Health Care Industry Cybersecurity (HCIC) Task Force, calls for increased information sharing among government and industry stakeholders, particularly to small and rural organizations. However, often these smaller entities do not have the resources to hire or maintain cybersecurity professionals that can fully utilize the information they receive. How do you propose that we close the cybersecurity labor gap in conjunction with the increased sharing of information?

3. While we see tremendous advantages to electronic health records in terms of efficiencies and patient safety, we have seen case after case of cyber breaches. This is often due to poor cyber hygiene and the use of legacy systems that are vastly outdated. In fact, according to the HCIC Task Force Report, a majority of the health care sector didn't make financial investments in cybersecurity until approximately five years ago.

    a. How can we increase education and training for health professionals to improve cyber hygiene?

    b. What obstacles exist to implementing updated systems across the health sector?

4. It is apparent that most of the data breaches we are seeing and what is being reported on are starting at the end user devices and then escalating across an organization's network. This is very concerning as attackers are focused on the human element and utilizing known vulnerabilities to disrupt so many organizations. Given the criticality of these devices in the patient care setting, is this issue more systemic at the user level, or is there something we can do to minimize the risk and impact related to the end user devices?

5. We are seeing more and more connected medical devices as part of the Internet of Things. Our assumption is that each equipment maker will have their own set of servers, data, and possible connections to the cloud.

    a. How can we ensure that as these devices are added they will be secure, stay secure given the known issues with patching, and ensure that if one of these devices is compromised it will not allow every other connected medical device to be compromised?

    b. Should a "bill of materials" accompany every device or health IT product to ensure integrity of composition?

6. What is the authority for HHS to support the Healthcare Cybersecurity and Communication Information Center (HCCIC) and foster the sharing of critical threat information when the National Cybersecurity Protection Act of 2014 (NCPA) and the Cybersecurity Act of 2015 (CISA) Section 102 establishes the National Cybersecurity and Communications Integration Center (NCCIC) to perform these functions?

The Honorable Susan Brooks

1. While we see tremendous advantages to electronic health records in terms of efficiencies and patient safety, we have seen case after case of cyber breaches. Given the sensitivity of health records and data what actions need to be taken to properly protect these records and systems in a manner that is more secure than the networks of today?

2. Looking at the WannaCry ransomware outbreak, experts from the health care and cybersecurity sectors have said that the health care sector remains vulnerable to infections like this one. They point to issues such as poor patch management, legacy systems, and a lack of expertise in the sector as root causes of the problem. These issues are also identified in the Task Force report,

along with suggestions regarding how to address them. What is HHS doing today help the health care sector address these lingering threats?

   a. Are there obstacles that HHS has identified in recovering from this outbreak, and preparing for the next?

   b. What are they, and what is HHS doing to address those obstacles, or help the sector address them?

3. It seems apparent that most of the data breaches we are seeing and what is being reported on are starting at the end user devices and then escalating across an organization's network. This is very concerning as the attackers are focused on the human element and utilizing know vulnerabilities to disrupt so many organizations. Given the criticality of these devices in the patient care setting, is this issue more systemic at the user level or is there something we can do to minimize the risk and impact related to the end user devices?

4. As healthcare is looking for greater interoperability and the ability to seamlessly share data in a secure manner, what can be done to ensure that the data remains accurate and secure? Can the security of the transport of the data be guaranteed to not be compromised and if so what are some of the methodologies that can be deployed to keep that data secure?

5. We are seeing more and more connected medical devices as part of the internet of things. Our assumption is that each equipment maker will have their own set of servers, data, and possible connections to the cloud. How can we ensure as these devices are added they will 1) be secure 2) stay secure given the know issues with patching even traditional servers; and 3) ensure that if one of these devices is compromised that they do not allow every other connected medical device to be compromised?

The Honorable Tim Walberg

1. The hearing focused heavily on specific actions that HHS is taking, or should take, to improve health care cybersecurity, such as setting up the HCCIC or reviewing conflicting and confusing regulations. However, there is one very important issue that I don't think was discussed, and that's this: HHS can create the best cybersecurity resources, or the most streamlined regulatory environment, but if there aren't qualified, knowledgeable experts at these health care organizations that truly understand how to leverage them, they won't be effective. And according to the Health Care Industry Cybersecurity Task Force report, the health care sector is severely lacking qualified cybersecurity experts.

   a. Is HHS concerned about the lack of cybersecurity experts available to health care organizations?

   b. How does HHS plan to help industry address this shortage of qualified personnel?

The Honorable Ryan Costello

1. Over the past few years we have heard of several significant data breaches and unauthorized exfiltration of sensitive data across the government. While we are addressing our failures in the

past by enhancing our network and perimeter security, it appears that we are failing to address how we protect sensitive data within and outside our networks.

a. What steps/measures are you considering that are data-centric, as opposed to perimeter-based or otherwise, to ensure the privacy and security of data and preventing data exfiltration in the event of an intrusion?

b. What is your ability to (cryptographically) protect data at rest, in transit, and in use?

c. Do you have any mechanism to protect sensitive data from improper access by highly privileged users such as system administrators?

d. What ability do you have to detect improper data access by authorized users (*i.e.*, in an anomalous and possibly malicious manner)? Do you have proactive capabilities in this area, or only after-the-fact, forensic capability (or neither)?

e. Do you have the ability to share sensitive data across your organizational boundary with authorized recipients and still protect it?

f. How do you measure use of or attempts to use data – successful or otherwise - that has been the subject of a breach, as opposed to simply reporting the number of records that have been breached?

g. What monitoring tools and technologies do you use in advance of learning about a breach to detect and anticipate breaches and attempts to gain access to data?

2. Whether intentional or unintentional, users typically resist additional security steps and friction in their workflow and often are the target of malicious attacks.

a. Do you have the ability to transparently encrypt and decrypt data for common file types that your users work with?

b. When you encrypt data, do you do this from the moment of creation to the moment of consumption, or do you do this only on backend systems (encrypted database or hard drive disks)?

c. Can you revoke access on a granular level to specific documents, people, etc. after the document has left your control (e.g. without having to recall the file and retransmit a new version)?

3. In your role as Co-Chair of the Health Care Industry Cybersecurity Task Force, and as a Chief Information Security Officer at CMS, have you looked into the fact that many servicers of medical equipment are unknown to the federal government and not under federal requirements to meet standards for servicing?

4. Currently, only the original equipment manufacturers (OEMs) are required to report to the FDA and meet federal quality servicing standards.

a. How can CMS be assured that critical equipment is being patched against cybersecurity problems if there is no window into all providers of service?

b. What is CMS doing to ensure that such providers are able to meet cybersecurity needs as they access highly technical, network-based equipment?