June 20, 2016

Mr. Josh Corman
Director
Cyber Statecraft Initiative
Atlantic Council
1030 15th Street, N.W.
Washington, DC 20005

Dear Mr. Corman:

Thank you for appearing before the Subcommittee on Health on May 25, 2016 to testify at the hearing entitled "Examining Cybersecurity Responsibilities at HHS."

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 July 5, 2016. Your responses should be mailed to Graham Pittman, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to graham.pittman@mail.house.gov.

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

Sincerely,

Joseph R. Pitts
Chairman
Subcommittee on Health

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

Attachment

Attachment — Additional Questions for the Record

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.

A1: As an outside citizen, I lack meaningful visibility into HHS's program. My expertise and context as a panelist was to contrast with all of my work with CISOs through the private sector and through my teaching for the CISO program at Carnegie Mellon Univesristy's Heinze College. Anything I offer to this question would be speculative.

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

A2: Every program and culture are different and involved trade-offs. My testimony was largely pointing at the difficulty in a CISO being fairly heard and acted upon. If there is a structural conflict of interest in place like reporting to a CIO – who has different (and often conflicting) incentives and measurements. As a baseline, the EO/NIST CyberSecurity Framework outlines several important program elements - but not necessarily the efficacy of its activities/controls on their own or as implemented in context.

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?

A3: Again, ss an outside citizen, I lack meaningful visibility into HHS's program. Anything I offer to this question would be speculative. One promising and emerging practice I'd like to see considered by HHS and other parts of the US Government is the addition of Coordinated Vulnerability Disclsoure Programs. These proven programs from the private sector (an exemplar is Microsoft's BlueHat program) invite independent, 3rd party researchers to looks for and report vulnerabilities to the affected party. This spring, the US Pentagon did a pilot "Hack the Pentagon" Boug Bounty to find weaknesses it's websites. Such programs allow more scalable detection and discrete remediation of things the formal security programs may have missed. NTIA within Commerce has held a mutli-stakeholder program over the past year to capture and promote best practices for such programs. Additionally, the US FDA within HHS has encouraged Medical evice Manfucaturers to offer such Disclsoure Programs to maiuntain public trust and enhance Patient Safety.

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;

   A4a: Ultimate responsibility for the security of both HHS Infrastructure and the Confidentialy, Integrity, and Availability of important information and services – required to fulfill it's duties to the government and taxpayers. Make ultimate decisions where trade-offs are required between CIO and CISO – in these regards.

   - The HHS CIO;

   A4b: Factor all CyberSecurity objectives into the selection, deployment, and maintaininace of IT purchases and 3rd party relationships – in consultation with the CISO. CIO and IT teams often share operational responsibilities for instrumentation and monitoring of IT when it comes to security issues – and participate in disaster recovery, business continuity planning and exercises (for example).

   - The HHS CISO;

   A4c: Develop CyberSecurity Objectives, Programs, Policies, and Measurements, and Risk Management Functions – in consulation with executive and agency stakeholders – to support their missions. Enable, train, and consult with key stakeholders in the executive team and division leads to meet mutual targets.

   - Any other officials (such as the General Counsel, CFO, etc.).

   A4d: Consult with the CISO to identify top risk priorities and mission requriements. Bring your power and influence in support of Cyber Security and Risk Management Objectives. Ensure your parts of the organization internalize and act in accordance with thee objectives. As I indicated in my prio written testimonies, different Executive Stakeholders express different aspects of a complete program. E.g. General Counsel cares about keeping secrets secret. Procurment can enforce security criteria upon 3rd party suppliers. Etc.

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?

A5: Given that the spirit of the H.R. 5068 was (in part) to remove any conflict of interest that affected the CISO's ability to objectively perform its required job functions, I would think this position should not be a political appointee.