Attachment – Answers: 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.**

HHS like other Departments of the Government must be compliant with the Federal Information Systems Management Act (FISMA) which uses as its basis the National Institute of Standards and Technology Cybersecurity Framework for implementing and measuring the effectiveness of its efforts to protect information. HHS with its multitude of program responsibilities and diverse information ecosystem is likely subject to many other different information security standards as well such as SAMHSA, FDA requirements, the Common Rule, etc. The NIST Cybersecurity Framework provides an effective structure for addressing the Department's many diverse regulatory security requirements. HHS has various governance structures like the CIO Council and the CTO Council where privacy and security issues are raised and vetted with senior leadership. The HHS CISO sits on the CTO Council. I am sure, but am not privy to, the existence of other policy elements of their program, but they have the basic elements of policy and framework that support the necessary procedure and processes required to manage a cybersecurity program.

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

By using the NIST Cybersecurity Framework and the NIST Guides for information security the HHS assures that it is following a well researched and up to date set of standards and guidelines for managing cybersecurity. Like any organization managing a dynamic program with multiple elements subject to change they should be constantly reviewing their program, their policies, their procedures and processes against the latest guidelines and alerts published by NIST to insure their program is as up to date as possible. NIST publishes specific guidelines addressing areas such as encryption, cloud services, third party relationships, etc. and these should also be consulted when appropriate. Information security is a constantly changing state with influences from technology, the threat, operations and the environment that must be constantly monitored and addressed.

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?**

I am not aware of any policies, procedures or processes that HHS should consider reforming or removing that supports their program. However HHS does have responsibility for overseeing privacy and security in healthcare and the businesses that handle protected health information under the Health Information Portability and Accountability Act (HIPAA) and its follow on legislation the HITECH Act and the Omnibus Rule. The HIPAA Security Rule, first conceived in the late 1990s and implemented in 2003 is woefully inadequate to meet the needs of the current cybersecurity environment we live and operate in today. This rule has not undergone revision since it was introduced, yet every other credible security standard whether NIST, ISO 27000, ITIL, etc. has been revised at least three or four times between 2003 and today. If there is a policy standard that HHS needs to address it is the HIPAA Security Rule. There is also I believe already a basis for doing this as many health systems already know the HIPAA Security Rule is not enough and have adopted the NIST standards to proactively improve the effectiveness of their program. To date more than 60% of healthcare follow or use NIST as the basis for their cybersecurity program. HHS should consider adopting the NIST Cybersecurity Framework across the board, not only for its own internal purposes, but for the industry as a whole to raise the standard of healthcare security.

In general organizations that place requirements on their fiscal structures for considering security in investment decisions tend to focus more on data security. The HHS CIO Council Charter describes that body's responsibilities for overseeing information technology investments and its relationship to the HHS Information Technology Investment Review Board (ITIRB) and the HHS Capital Planning and Investment Control (CPIC) policy. What is conspicuously absent, but is address in the CTO Council Charter, is reference to cybersecurity when making or reviewing information technology investments. Cybersecurity should be present at all levels of the governance structure in the Department to include the CIO Council.

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;**

The Secretary of Health is and should be ultimately responsible for the protection of Departmental information assets and for promoting effective cybersecurity protections in the nations healthcare industry. They should be responsible for appointing a competent individual to serve as the HHS CISO to advise them and the leadership of HHS on cybersecurity policy and measures necessary to carry out the information security mission of the Department. They should be responsible for reporting to the Administration and to Congress on whatever basis deemed necessary regarding their

Departments efforts and status with respect to cybersecurity preparedness. They should be responsible for ensuring an effective governance structure is out in place throughout the Department to provide oversight, accountability, direction and resource support.

- **The HHS CIO;**

The HHS CIO should be responsible for implementing and delivering the necessary information services to support the operations of the Department in a manner that promotes the protection of information assets and sensitive information. They should implement the security technologies that are required to security the enterprise effectively and support security operations. They should ensure that information assets are implemented in accordance with the Departments cybersecurity policies. They should ensure that all information technology personnel are trained on the security skills required for their position and those with specific security responsibilities receive specialized training to perform their roles effectively. They should work collaboratively with the CISO to ensure that all information assets are selected, procured, implemented, tested, maintained and retired in an appropriate manner to ensure the protection of the Departments assets, operations, personnel and information.

- **The HHS CISO;**

There are many well written CISO position descriptions that detail the role and responsibilities of the CISO in an organization. What I feel is germane for this discussion is the importance of the role as the chief advisor on cybersecurity matters to the Secretary HHS. The HHS CISO is the principle with primary responsibility for overseeing the on-going activities and development, implementation, and improvement of the Department's information assurance program and compliance with Federal regulations. The HHS CISO in collaboration with the HHS CIO is responsible for ensuring that Departmental information assets and data are protected adequately. Serves as the primary cybersecurity advisor to the Secretary HHS and collaborates with other CISOs across the Federal government and industry. Maintains in depth knowledge of cybersecurity matters, standards, frameworks, technologies to inform information technology strategy and security controls. Is or appoints a member to the CIO and CTO Councils. The CISO should be designated as the senior official responsible for accrediting HHS information assets as having met and continuing to meet Departmental and Federal mandates for cybersecurity.

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

First, let me say that every other official and employee ought to have information security responsibilities articulated in their position descriptions if for no other reason than to convey their responsibilities as system and data users. There are a number of other important positions from a policy perspective to ensure effective cybersecurity. Those include the General Counsel (GC), Human Resources, the Chief Financial Officer (CFO), the Chief Procurement Official, the Chief of Physical Security. Effective cybersecurity relies on an integrated ecosystem of controls and behaviors to be successful. These other

principles in the Department are important by supporting, but not limited to, understanding and articulating risk, personnel selection, screening, accountability and training, supporting effective budget development/defense, ensuring acquisitions involving information technology are reviewed before purchased and complimentary controls are in place to physically protect information assets and data. Information security is a cultural phenomena that requires action, input, support, vigilance, etc. from the bottom up and the top down in every organization.

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.

Would the position be more effective if it wasn't a presidential appointment?

Personally I do not believe this position needs or should be a presidential appointment. The Secretary should be able to appoint his or her CISO in the same manner as they appoint the CIO. If we use the rationale that we need the CISO position appointed as a presidential appointment to ensure effective cybersecurity then we would need to treat the CIO position the same way. They are both critical to the success of the program. I believe that what is more important is the description of the position and the qualifications of the appointee.