HIMSS
transforming health through IT

33 West Monroe St, Suite 1700
Chicago, IL 60603-5616
Tel 312 664 4467
Fax 312 664 6143
www.himss.org

July 5, 2016

The Honorable Joseph R. Pitts
Chairman
Subcommittee on Health
House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Pitts:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), thank you for the opportunity to testify before the Subcommittee at the May 25, 2016 hearing entitled "Examining Cybersecurity Responsibilities at HHS." HIMSS and our members look forward to working with you to ensure the healthcare sector has the tools, resources and structures in place to protect patients and their information from growing cyber threats.

Attached please find my responses to the follow-up questions submitted for the record. If you would like additional information, please contact me at sbburch@himss.org or 703-562-8847.

Sincerely,

Samantha Burch
Senior Director, Congressional Affairs
HIMSS North America

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

The Honorable Joseph R. Pitts

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.

The following information is based on the "Annual Report to Congress Federal Information Security Modernization Act (OMB, March 18, 2016)":

Anti-Phishing Defense and Other Defenses

- Web content filtering
- Quarantining or blocking messages to protect individual user machines and the system at large from the consequences of opening email messages infected with viruses or other nefarious programming

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

HHS should adopt a department-wide, enterprise-level cybersecurity governance framework, which is fully implemented across the organization.

Based on the deficiencies cited in the March 2016 HHS OIG Report, "Review of the Department of Health and Human Services Compliance with the Federal Information Security Modernizations Act of 2014," the framework should have the following components:

- HHS' senior management should develop policies that address its risks with a "whole of organization" approach (i.e., taking into account risks from operational, legal, financial, and/or reputational perspectives and the confidentiality, integrity, and availability of information and assets). Additionally, regular accurate and thorough risk assessments should be conducted across the enterprise, taking into account people, processes, and technology within the enterprise and with external partners (to the extent such visibility exists). Based upon the results of the risk assessment, these results can be used to inform the policies senior management develops.
- HHS' mid-level management should add standards, baselines (i.e., minimum requirements), guidelines, and procedures to such policies. Security professionals can assist with adding such information.
- HHS' security professionals should implement the policies and associated standards, baselines, guidelines, and procedures.
- HHS' users should comply with such policies.
- At each level cited above, there should be a consistent approach to accountability to ensure compliance and full implementation of such policies. There should be formally defined, consistently applied sanctions for violations of such policies.
- At each level cited above, there should be a clear, consistent, and formalized approach to documentation. Not having a formalized documentation process and having appropriate and detailed documentation may expose HHS to potential liability for lack of due care and/or due diligence.
- At each level cited above, there should be a clear, consistent, and formalized approach to tracking and monitoring of initiatives and activities across the enterprise.

- Additionally, there should be oversight at each of these levels. What the policies state and what is done in practice should be made uniform across the Department.

HHS' senior management should provide oversight over the implementation of the policies.

- Contingency planning and disaster recovery should be addressed with a consistent, formalized approach. This should also be driven by senior management, fleshed out by mid-level management, and implemented by appropriate personnel.
- Awareness and training of workforce members across the enterprise should be mandatory to ensure that everyone understands and complies with policies, procedures, guidelines, and baselines, as appropriate.
- Finally, with all of these changes, the changes should be controlled (or managed) to control the risk (i.e., change management).

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?

The addition or enhancement of information sharing within the organization and with external parties (as emphasized in Section 405 of the Cybersecurity Act of 2015) should be encouraged, facilitated, and implemented in a formal enterprise-wide policy. Information can be shared with regard to obstacles or barriers in implementing policy or questions about how to uniformly apply policy. This feedback can be valuable and senior management and middle management, as appropriate, can modify policies and other items to make such tasks more feasible.

Information can be shared with regard to privacy and security incidents to more effectively mitigate incidents that occur. When a privacy or security incident does occur, HHS can become more resilient by using lessons learned from the incident and improving or revamping people, processes, and technology.

4. Please describe the responsibilities and authorities that you believe the following HHS officials should have with regards to cybersecurity:

Based on HIMSS' extensive experience working with private sector healthcare organizations, we the following responsibilities and authorities could apply to the roles identified below within HHS.

- **The Secretary of Health;**
    - Establish cybersecurity as a priority for the enterprise by ensuring that resources are appropriately allocated;
    - Facilitate the changing of the culture about cybersecurity throughout the enterprise;
    - Review regularly updated information about the state of cybersecurity and impacts on the Department; and,
    - Review of metrics that show progress with regard to the cybersecurity program
    - Provide ultimate oversight and accountability for the cybersecurity program and initiatives.

- **The HHS CIO;**
    - Ensure that technology is functional, operating correctly, and supports the operations of the Department;
    - Oversee the IT budget;
    - Oversee the IT lifecycle of software, hardware, and other resources;
    - Oversee the selection, vetting, and procurement of technology;
    - Oversee the inventory of IT assets and resources;
    - Oversee relationships with third party partners, vendors, and others relevant to IT operations;
    - Provide oversight to implementation of IT operational policies and procedures and ensures consistency across divisions, offices, and also throughout the enterprise; and,
    - Ensure appropriate and consistent documentation.

- **The HHS CISO;**
    - Oversee cyber threat, vulnerability, and mitigation information sharing with other Federal agencies and within the enterprise;
    - Oversee the assessment and management of risks;
    - Oversee physical, technical, and administrative security safeguards;
    - Oversee assessment and management of risks (including in view of the direction and guidance of senior management);
    - Oversee relationships with third party partners, vendors, and others relevant to cybersecurity;
    - Oversee the facilitation of information sharing about cyber threats, vulnerabilities, and mitigation information with private sector healthcare entities;
    - Oversee development of policies, procedures, baselines, and guidelines from a cybersecurity perspective;
    - Confer with senior privacy officials to safeguard the privacy of confidential or sensitive information, personally identifiable information, or classified information;
    - Confer with senior privacy officials about the handling of incidents;
    - Ensure that qualified cybersecurity personnel are hired and retained throughout the enterprise; and,
    - Develop, executes, and manages cybersecurity awareness and training programs for the entire workforce across the enterprise.

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

The General Counsel should work with other C-suite executives and the Secretary to ensure compliance with laws, regulations and contractual requirements. The General Counsel and staff also should also take due care and due diligence to ensure targets for enterprise-wide cybersecurity program are met and continuously monitored (including with regard to FISMA targets).

The CFO should ensure the development, execution, and oversight activities involving the budget and financial performance should include cybersecurity. The CFO should work with the CISO and CIO to ensure that all relevant factors are taken into consideration.

5. **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?**

Yes, the position would be more effective for a number of reasons including:

- The person would not be time-limited and policy, activities, and initiatives would not be rushed because of that time limitation.
- A person who is a permanent employee would afford continuity and less disruption to the organization.