Testimony from the Department of Health and Human Services on

Cybersecurity in the Health Care and Public Health Sector

Before the

United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

June 8, 2017

Chairman Murphy, Ranking Member DeGette, and Members of the Subcommittee, thank you for inviting the Department of Health and Human Services' (HHS) representatives with the HHS Office of the Chief Information Office and the HHS Office of the Assistant Secretary for Preparedness and Response and the Health Care Industry Cybersecurity Task Force Co-Chair to testify on how HHS and its partners are addressing cybersecurity. HHS is committed to working together across the Department and with private sector stakeholders to help combat cybersecurity threats.

In the past five years, few infrastructure issues have challenged the health care and public health sector (HPH sector) more than cybersecurity. Within our modern system of health care, nearly everything is connected through a system of systems, from dialysis machines to electronic health records. Cybersecurity is both a direct and a secondary threat. It can impact everyday patients and health care delivery by locking down access to power, important medical information, and life-saving equipment. It can also exacerbate an existing emergency when hospitals, EMS, and emergency first responders are already working a frantic pace to save lives and cannot afford to lose access to communications or risk further delays in their response.

Since 2014, the HPH sector has been hit with a wave of health care information breaches, compromising the personal information of individuals. In 2016, we started to see a rise of ransomware attacks against the HPH sector. In these attacks, computer malware was used to lock up the files of victim health care organizations, while criminals demanded a ransom payment in exchange for access to be returned. These attacks shifted the threat landscape considerably, as they no longer threatened just personal information but also the ability of health care organizations to provide patient care.

The Department has a wide range of health care and public health responsibilities that touch on nearly every corner of the health care sector, ranging from the Food and Drug Administration's role in medical devices to the Centers for Medicare & Medicaid Service's role in electronic health records to the Center of Disease Control and Prevention's role in protecting public health. The complexity and size of the Department's mission and important role in coordinating cybersecurity preparedness with the private sector led to HHS's designation as the Sector Specific Agency (SSA) for the health care and public health (HPH) sector through the Presidential Policy Directive 21 (PPD-21). As an SSA, HHS, in coordination with the Department of Homeland Security (DHS), is responsible for working collaboratively with public and private sector organizations in the HPH sector to increase the security and resilience of the sector against any hazards it may face. The HPH sector is large and diverse and the risks faced by the sector are diverse as well. The risks include cyber-attacks as they could threaten the ability of health care organizations to provide care.

Extensive partnerships across HHS, the rest of the federal government, and the private sector have helped HHS to leverage the expertise needed to combat this growing threat. Most recently, HHS through its Office of the Assistant Secretary for Preparedness and Response (ASPR) was integral in the HPH sector-related response to the WannaCry ransomware attack which impacted dozens of hospitals in the United Kingdom. The Department, in coordination with DHS's National Cybersecurity and Communications Integration Center (NCCIC), crafted an immediate response to engage the broader health care sector and ensure that information technology (IT) security practitioners had the information they needed to protect against, respond to, and report, WannaCry intrusions on their networks. While this was the first time HHS had organized itself in this way for a cybersecurity incident, we believe that it has set a standard on how to manage cybersecurity incidents in this era of heightened consequences and in support of the National Cyber Incident Response Plan.

HHS Cybersecurity Leadership and Cybersecurity Working Group

Under Executive Order 13800, the Secretary has overall accountability for the Department's cybersecurity risk management. The HHS Cyber Threat Preparedness Report, required by the *Cybersecurity Act of 2015*, identified the HHS Deputy Secretary as the official who has overall leadership within the Department for cybersecurity. The HHS Deputy Secretary in turn designated the HHS Deputy Chief Information Security Officer as the Senior Advisor for Cybersecurity. The Deputy Chief Information Security Officer is also the Chair of the HHS Cybersecurity Working Group. The HHS Cybersecurity Working Group is the principal forum for coordinating cybersecurity support and response across all HHS Operating Divisions and Staff Divisions, to better align resources to provide communications and support. This critically important step will leverage HHS capabilities and outreach to help the HPH sector improve its preparedness for, and response to, security incidents now and into the future. The Senior Advisor for Cybersecurity will align and coordinate internal stakeholders to collaborate with the private sector, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) and the U.S. Department of Homeland Security (DHS) to develop voluntary guidelines to support adoption of the NIST Cybersecurity Framework, and support HPH sector risk reduction and resilience.

Healthcare Cybersecurity Communications Integration Center (HCCIC)

HHS supports the HPH sector through the establishment and operation of the Healthcare Cybersecurity Communications Integration Center (HCCIC). The HCCIC has three high level goals:

- Strengthen engagement across HHS Operating Divisions;
- Strengthen reporting and increase awareness of the health care cyber threats across the HHS enterprise; and
- Enhance public-private partnerships through regular engagement and outreach.

The HCCIC was an integral part of ASPR's coordinated response to the recent WannaCry incident. It provided analysis on the WannaCry threat and its impact on health care. The HCCIC design and concept of operations was developed with the aid of the Carnegie Mellon University Software Engineering Institute and is modeled on the design of the National Cybersecurity Communications Integration Center.

Health Care Industry Cybersecurity Task Force Report

In the *Cybersecurity Act of 2015*, Congress required the establishment of the Health Care Industry Cybersecurity Task Force to review and analyze challenges the health care industry faces when securing and protecting itself against cybersecurity incidents, whether intentional or unintentional.

The Secretary of Health and Human Services in consultation with the NIST Director and the DHS Secretary assembled a diverse group of industry representatives to discuss these issues, consistent with the requirements outlined in the Act. Industry participation in the Task Force brought to light critical areas for discussion.

Twenty-one Task Force members contributed to this effort, including seventeen from private sector organizations. The Task Force identified a wide range of threats that affect the health care industry. In doing so, it relied on information gathered during public meetings, briefings and consultations with experts on a variety of topics across health care and other critical infrastructure sectors, internal Task Force meetings, and responses to blog posts.[1]

Following a year of discussion within the Task Force and information gathered from external stakeholders and subject matter experts across the health care industry and other sectors, the Task Force identified six high-level imperatives under which to organize the recommendations and action items. The Task Force's report[2] and recommendations are consistent with the policies and directives outlined in the Presidential Executive Order on Strengthening the Cybersecurity of

[1] The Act identifies members of the health care industry to include: health plans (including health insurance companies), health care clearinghouses, and health care providers; patient advocates; pharmacists; developers of health information technology; laboratories; pharmaceutical or medical device manufacturers; and other additional stakeholders in the definition of health care industry stakeholders.

[2] https://www.phe.gov/Preparedness/planning/CyberTF/Pages/default.aspx

Federal Networks and Critical Infrastructure, released on May 11, 2017.[3] Both the Executive Order and Task Force highlight the importance of effective risk management and the need for cyber security to be integrated into risk management assessments across agencies.

The six imperatives outlined by the Task Force are:

1. *Define and streamline leadership, governance, and expectations for health care industry cybersecurity*. Acknowledging the wide array of stakeholders and the diversity of needs across the health care industry the Task Force made several recommendations. The Task Force recommended the creation of a "cyber leader" role within HHS to coordinate activities and serve as a single focal point for industry engagement across regulatory and voluntary cybersecurity programs. The Task Force found that HHS needs to make the discussion, oversight, and engagement around cybersecurity clearly and consistently messaged. In addition the Task Force made additional recommendations to help streamline and harmonize cybersecurity efforts and the sharing of best practices across the industry. The Task Force paid particular attention to the needs of small and medium sized organizations, which have unique needs and different capabilities as compared to larger organizations.

2. *Increase the security and resilience of medical devices and health IT.* This imperative addresses the legislative request to look specifically at the unique cybersecurity challenges of medical devices and electronic health records. This imperative takes a total product lifecycle approach, recommending a mix of regulation, accreditation, information sharing, and voluntary development and adoption of standards to promote system security from product design and development through end of life. The Task Force recommends that HHS evaluate opportunities

[3] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

for strengthening public/private relationships and leverage the progress already made by associations and groups that have brought the private sector together around cybersecurity challenges.

3. *Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.* The Task Force outlines the major workforce challenges facing health care information technology and cybersecurity, especially among small, rural, and other lesser-resourced organizations. It recommends steps to enhance cybersecurity leadership in organizations, develop the nation's health care cybersecurity workforce, and create options for organizations to gain efficiencies by leveraging shared cybersecurity services.

4. *Increase health care industry readiness through improved cybersecurity awareness and education.* This imperative focuses on increasing the cybersecurity posture within organizations by raising awareness among corporate leadership, educating employees on the importance of cybersecurity, and empowering patients to make better choices related to the security of their personal health information. The Task Force recommends that HHS and industry partners promote cybersecurity awareness across health care.

5. *Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure.* This section focuses on the significant problem of health care intellectual property theft related to areas such as clinical trials, drug and device development, big data applications, and general health care business operations. It recommends activities to increase the industry's understanding of the scope of the problem and the economic and other risks of continuing intellectual property loss.

6. *Improve information sharing of industry threats, risks, and mitigations.*

Recommendations under this imperative focus on the sharing of cyber threat information among government and industry partners. The Task Force recommends general principles to follow in the establishment of cyber threat information sharing systems in health care, with a focus on ensuring that curated and actionable information reaches small and rural organizations.

Conclusion

HHS's cybersecurity mission is a combined national response requiring broad collaboration across the Department, the government and private sector partners. The Department is committed to a safe, secure, and resilient cyber environment that promotes cybersecurity knowledge, innovation, confidentiality, and privacy in collaboration with public, private, and international partners. Thank you again for the opportunity to testify and we look forward to your questions.