June 8, 2017

Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity

Subcommittee on Oversight and Investigations.,Committee on Energy and Commerce, United States House of Representatives, One Hundred Fifteenth Congress, Second Session

---

Hearing Contents:

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

Witnesses

Mr. Emery Csulak
Chief Information Security Officer and Senior Privacy Official, Centers for Medicare and Medicaid Services, Co-Chair, Health Care Industry Cybersecurity Task Force
View Testimony

Mr. Steve Curren
Director, Division of Resilience, Office of Emergency Management, Office of the Assistant Secretary for Preparedness and Response, U.S. Department of Health and Human Services
View Testimony

Mr. Leo Scanlon
Deputy Chief Information Security Officer, U.S. Department of Health and Human Services
View Testimony

Compiled From*:

U.S. House of Representatives Committee Repository

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

Opening Statement of The Honorable Tim Murphy
Subcommittee on Oversight and Investigations
Hearing on "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity"
June 8, 2017

(As prepared for delivery)

We are here today to continue our examination of cybersecurity in the health care sector. As we discussed at our hearing in April about the role of public-private partnerships, cybersecurity in this sector ultimately comes down to patient safety. And we got a glimpse just weeks ago at what a large-scale cyber incident could do to the health care sector—including the impact on patients—during the WannaCry ransomware event. Today, we turn to the role of the Department of Health and Human Services (HHS) in health care cybersecurity.

Recognizing the critical importance of cybersecurity in this sector, two years ago, in the Cybersecurity Act of 2015, Congress asked HHS to undertake two evaluations—one evaluating the Department's internal preparedness for managing cyber threats, and a second done alongside industry stakeholders examining the challenges of cybersecurity in the health care sector. These evaluations are now complete, and give not only the Congress, but the entire health care sector, an opportunity to better understand the agency's approach to cybersecurity. The reports also allow us to establish a baseline for evaluating HHS' progress moving forward.

HHS's internal preparedness report sets out the roles and responsibilities of various HHS offices in managing cyber threats, among other information. For example, the report identified a single HHS official – the cybersecurity "designee" – as having primary responsibility for cybersecurity efforts across the agency. But what precisely does this mean, and how does this cybersecurity designee work with the eleven components identified by HHS as having cybersecurity responsibilities? In addition, the Committee has learned that many of the details may already be obsolete due to recent and ongoing changes in HHS's internal structure.

For example, HHS's creation of a Health Cybersecurity and Communications Integration Center (HCCIC), modeled on the National Cybersecurity and Communications Integration Center (NCCIC) operated by the Department of Homeland Security, could dramatically change how HHS handles cyber threats

internally. It is our understanding that the HCCIC will serve as a focal point for cyber threat information collection and dissemination from HHS's internal networks, as well as external sources. However, details about this new function remain limited. Therefore, how the HCCIC fits in to the Department's internal structure and preparedness, as well as its role with respect to private sector partners will be a focus of today's discussion.

The second report, released late last week, focuses broadly on the challenges of cybersecurity in the health care industry. This report reflects the findings and recommendations of the Health Care Industry Cybersecurity Task Force. The Task Force members were selected from a wide-range of stakeholders, including federal agencies, the health care sector and cybersecurity experts. The report does not mince words, broadly concluding that health care cybersecurity is in critical condition. The report identified six imperatives—such as defining leadership and expectations for the industry, increasing the security of medical devices and health IT, and improving information sharing within the industry—and made 27 specific recommendations. Many of these recommendations call on HHS to provide more leadership and guidance for the sector as a whole.

It is clear from these reports that there is much that HHS can and should do to help elevate cybersecurity across the sector. The importance of meeting this challenge head-on was illuminated in recent weeks by the widely-publicized WannaCry ransomware. Frankly, we are lucky that that United States was largely spared from this infection, which temporarily crippled the National Health Service in England. Doctors and nurses were locked out of patient records. Hospitals diverted ambulances to nearby hospitals and cancelled non-emergency services after widespread infection of the ransomware.

This incident was an important test of HHS's response to a potentially serious event and thus far, the feedback has been positive. Reports suggest that HHS took a central role in coordinating resources, disseminating information and serving as a nerve center for public-private response efforts. But this was just one incident, and HHS must remain vigilant. The WannaCry infection was not the first widespread cyber incident, nor will it be the last.

Therefore, a commitment to raising the bar, for all participants in the sector – no matter how large or small, needs to be embraced. This is a collective responsibility and HHS has an opportunity to show leadership and to set the tone. Because this is no longer just about protecting personal information or patient data. This is about patient safety.

I want to thank our witnesses for appearing today and look forward to learning more about HHS's efforts on this important topic. I now recognize the Ranking Member, Ms. DeGette, for her opening statement.

Opening Statement of Chairman Greg Walden
Subcommittee on Oversight and Investigations
Hearing on "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity"
June 8, 2017

Our lives continue to become more interconnected every day. This explosion of digital connectivity and information technology provides us with previously unimaginable convenience, engagement, capabilities, and opportunities for innovation.

For all its benefits, however, the digitization of our daily lives also comes with risk. The internet and information technologies are inherently insecure. With time, motivation, and resources, someone halfway around the world can find a way into almost any product system.

As the opportunities for attackers proliferate, the potential consequences of their actions are becoming more severe. As more products, services, and industries become connected to the digital world, we must acknowledge that the threat is no longer just data and information – it is public health and safety.

For the health care sector, these factors present a very real threat – and equally daunting challenge. As we witnessed with the recent WannaCry ransomware outbreak, portions of the National Health System in the U.K. had to turn away patients except for emergency care after vulnerable systems fell victim to the exploit.

WannaCry did not appear to be a targeted attack on health care, but the potential consequence of the exploit on health care – including patient safety – was far more severe. If this had been a more sophisticated exploit, or a targeted attack on the health care sector, the consequences could have been far worse.

The health care sector is starting to grasp this new reality but, as noted in the recent task force report, which we will discuss today, health care cybersecurity is in "critical condition" and requires "immediate and aggressive attention."

Which brings us to today's hearing. Clearly, the sector needs leadership. HHS is uniquely situated to fill this void. Historically, the Department has struggled to effectively embrace this responsibility, but that trend cannot continue.

More recently, HHS has started to demonstrate a commitment and focus to addressing the rampant challenges in health care cybersecurity. For example, the Department's actions in response to the WannaCry ransomware - coordinated through the newly established HCCIC - have generally received praise from the sector.

This and other recent actions are positive signs that the Department is heading in the right direction. But HHS has a long way to go to demonstrate the leadership necessary to inspire change across the sector. It needs to be open and transparent about who is in charge and provide clarity about the roles and responsibilities, not only internally but across the sector. They need to make sure that a small rural hospital not only knows exactly who to call, but also has access to the resources and information to keep their patients safe.

This hearing provides an opportunity for HHS to provide some much needed clarity about its internal structure, as well as outline its plan to elevate cybersecurity across the sector.

The sector is operating on borrowed time. The cyber threat is spreading and, left unchecked, it will pose an increasingly greater threat to public health.

Opening Statement of the Honorable Michael C. Burgess, M.D.
Subcommittee on Oversight and Investigations on
"Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity"
June 7, 2017

Good morning. Cybersecurity in the health care sector is a timely topic that has real, physical consequences. In almost three decades as a practicing physician, ransomware was never an issue I faced. Now, the threats posed by malicious actors are almost universal across the sector due to legacy systems, poor cyber hygiene, and a severe shortage of qualified cybersecurity professionals.

Most cyber attacks have the potential to cause real harm, depending on the severity and target. However, in health care cybersecurity, it is a certainty. Anytime information in the health care and public health sector is compromised, it poses a risk to providers, patients, and all those who serve and supply them.

The recent WannaCry ransomware infected thousands of computers across the world and severely impacted the health care sector in the United Kingdom. While the U.S. health sector was largely spared from this paralyzing malware, some organizations continue to deal with the effects of trying to eradicate this virus from their systems. The ease with which WannaCry was able to infect so many systems is alarming – and it was entirely preventable. While this particular malware only sought to lock information until a ransom was paid, the threshold remains low for more malicious actors to access critical health systems. We must work to acquire the cyber expertise, resources, and structure to combat such vulnerabilities.

The report produced by the Health Care Industry Cybersecurity task force is a step in the right direction in improving our ability to prevent and respond to cybersecurity

events. The report also identifies the challenges posed by the health care and public health sector in maintaining security across unique platforms and devices that must all work in concert to enable accurate and timely patient care.

This is even more important when considering that health information isn't something you can easily change, such as a credit card or phone number. Your health information is your information for life, and the integrity of this data is paramount to protecting patient safety. Can you imagine the consequences of altering a person's blood type, allergies, or disease diagnosis in a system relied up on by providers to treat patients?

Overall, the health care and public health sector has improved its ability to manage cybersecurity events, including HHS' management of the WannaCry malware that resulted in minimal effect on U.S. health organizations. But the balance between securing important data and protecting patient privacy

needs continuous evaluation and adjustment. Is there a point where information sharing creates more vulnerability by identifying entities as targets of attack? What happens when health care organizations limit reporting of breaches or the sharing of information for fear of losing customer confidence or becoming a target? How do we increase the availability of cybersecurity professionals in the health sector? I look forward to discussing these and other issues with the witnesses today. Thank you.

COMMITTEE ON
ENERGY & COMMERCE
DEMOCRATS
RANKING MEMBER FRANK PALLONE, JR.
NEWS

FOR IMMEDIATE RELEASE
June 8, 2017

CONTACT
CJ Young — (202) 225-5735

Pallone: We Need to Up Our Game Against Cyberattacks

"We must make sure that HHS has the resources it needs to develop and implement a robust cybersecurity strategy"

Washington, D.C. – *Energy and Commerce Ranking Member Frank Pallone, Jr. (D-NJ) delivered the following opening remarks at an Oversight and Investigations Subcommittee hearing titled, "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity:"*

Mr. Chairman, thank you for holding this hearing today.

This Committee has a long history of examining cybersecurity. The federal government continues to make progress toward addressing vulnerabilities in the health care sector, but it is clear that we still have a lot of work to do.

For example, the 2015 Anthem attack highlighted the need for all industry members to come together and find solutions to cyber threats. More recently, the "WannaCry" ransomware attack demonstrated that cyberattacks have real world consequences that can place patients at risk.

And now, with the interconnection of health records – and a network of connected medical devices – the threat of cyberattacks on critical parts of our health care infrastructure is ever-present.

While there is no single solution, it appears the Department of Health and Human Services (HHS) is making some traction in assisting its own agencies and private stakeholders in confronting cyber threats. We must make sure that HHS has the resources it needs to develop and implement a robust cybersecurity strategy—something I hope we can explore today.

Just this past week, an HHS task force released a long-awaited report that describes challenges and makes recommendations to address cyber threats facing the health care sector.

The task force determined that the health care sector must pay “immediate and aggressive attention” to cybersecurity. It also made a host of important recommendations for the health care industry and HHS to consider.

There are no easy solutions for the issues highlighted in the report. I look forward to hearing how the administration intends to address them – and, importantly, how this Committee intends to hold HHS accountable for progress, or lack of progress, on this issue.

I am also interested in learning about how HHS plans to develop its newly proposed Health Cybersecurity and Communications Integration Center, and what challenges it faces in establishing and operating it.

Finally, Mr. Chairman, I am interested in understanding whether HHS has the budgetary resources it needs to appropriately address its cybersecurity responsibilities. This includes efforts to prevent cyberattacks. It also includes the HHS’s responsibilities to hold regulated entities accountable, especially when those entities fail to protect the sensitive health care information that we trust them to safeguard.

In conclusion, Mr. Chairman, we need to up our game if we intend to defend against a growing number of cyberattacks facing the health care sector.

I am pleased to welcome our witnesses from HHS, and I look forward to hearing from them about how HHS can enhance our health cybersecurity. But that being said, I believe we still have a long way to go to improve our preparedness in this area, and I look forward to hearing how this Committee intends to hold HHS accountable moving forward.

Thank you and I yield back.

###

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.