NEAL R. GROSS & CO., INC.
RPTS SALANDRO
HIF159020

EXAMINING THE ROLE OF THE DEPARTMENT OF
HEALTH AND HUMAN SERVICES IN HEALTH CARE
CYBERSECURITY
THURSDAY, JUNE 8, 2017
House of Representatives
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
Washington, D.C.

The subcommittee met, pursuant to call, at 10:15 a.m., in Room 2322 Rayburn House Office Building, Hon. Tim Murphy [chairman of the subcommittee] presiding.

Members present: Representatives Murphy, Griffith, Burgess, Brooks, Collins, Walberg, Walters, Costello, Carter, Walden (ex officio), DeGette, Castor, Tonko, Ruiz, Peters, and Pallone (ex officio).

Staff present: Jennifer Barblan, Chief Counsel, Oversight and Investigations; Elena Brennan, Legislative Clerk, Oversight and Investigations; Katie McKeough, Press Assistant; John Ohly, Professional Staff, Oversight & Investigations; Jennifer Sherman, Press Secretary; Hamlin Wade, Special Advisor, External Affairs; Jessica Wilkerson, Professional Staff, Oversight and Investigations; Julie Babayan, Minority Counsel; Chris Knauer, Minority Oversight Staff Director; Miles Lichtman, Minority Policy Analyst; Kevin McAloon, Minority Professional Staff Member; Dino Papanastasiou, Minority GAO Detailee; Andrew Souvall, Minority Director of Communications, Outreach and Member Services; and C.J. Young, Minority Press Secretary.

Mr. Murphy. Good morning. Commencing a hearing here on the -- examine the role of the Department of Health and Human Services on health care cybersecurity. Welcome.

We are here today to continue our examination of cybersecurity in the health 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.

We had a glimpse of that just weeks ago at what a large-scale cyber incident could do the health care sector including the impact upon patients during the WannaCry ransomware event.

Today, we turn to the role the Department of Health and Human Services, HHS, has 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 cyberthreats and a second done alongside industry stakeholders examining the challenges with 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= internal preparedness report sets out the roles and responsibilities of various HHS offices in managing cyberthreats, among other information.

For example, the report identified a single -- HHS= official -- the cybersecurity designee assigning primary responsibility for cybersecurity efforts across agency. But what precisely does this mean and how does the cybersecurity designee work with the 11 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= internal structure.

For example, HHS= creation of a Health Cybersecurity and Communications Center, or HCCIC, modeled on the National Cybersecurity and Communications Integration Center, or NCCIC, operated by the Department of Homeland Security could dramatically change how HHS handles cyberthreats internally.

It is our understanding that the HCCIC will serve as a focal point for cyberthreat information, collection and dissemination from HHS= internal networks as well as external sources. However, details about this new function remain limited.

Therefore, how HCCIC fits in 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 focused 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 stakeholder including federal agencies, the health care sector and cybersecurity experts. And 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.

It 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 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 the 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 there and hospitals diverted ambulances to nearby hospitals and cancelled nonemergency services after widespread infection of the ransomware.

This incident was an important test of HHS= response to a potentially serious event and thus far the feedback has been positive. Reports suggested HHS took a central role in coordinating resources, disseminating information and serving as a nurse in the 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.

So I want to thank our witnesses for appearing today and look forward to learning more about HHS= efforts on this important topic.

I want to also say we recognize that this is a very, very serious threat and we will be asking more details about that later. But one that has had that impact upon the National Health Service in England, I shudder to think what happens here.

If we are talking about threats to patients= medical records, prescribing records, medical equipment, et cetera, none of this should be taken lightly. This is a very serious problem.

So I now want to recognize the ranking member, Ms. DeGette of Colorado, for her opening statement.

Ms. DeGette. Thank you, Mr. Chairman.

The country=s vital infrastructure is under attack by actors with malicious intent. We are constantly seeing new headlines about vulnerabilities and cyberattacks against our systems and these attacks are becoming more frequent and more sophisticated.

In the health care sector, cyberattacks are particularly devastating, obviously because they can harm patients. Just last month, as the chairman mentioned, WannaCry ransomware crippled information systems around the world.

Hackers infected an estimated 200,000 computers in more than 150 countries. For the systems affected in the health care sector, the WannaCry attack meant that patients could not get their prescriptions at pharmacies and doctors even could not conduct surgery in their hospitals.

Cyberattacks in this sector are unfortunately not a new problem. For example, in 2015 more than 113 million medical records were reportedly compromised by a cyber intrusion.

In one widely publicized case involving a health insurance company, the personal information of nearly 79 million people was compromises.

Cyberthreats have become a new reality that we must all face. Information systems connected to the internet are vital to the operation of our economy and our government. While this interconnectedness is essential, it brings vulnerabilities and unique challenges.

Just this last week, an HHS task force released a major report on how to address cyber vulnerabilities within the department and the health care sector.

This report identified many cybersecurity problems confronting the industry, the department and its multitude of health-related agencies.

These problems include a lack of cybersecurity expertise in the workforce, a reliance on outdated legacy equipment and a failure of certain organizations to address vulnerabilities that can harm patients.

Our witnesses from HHS today will speak about their ongoing efforts to address these threats both within the department and within the larger health care sector. I am also aware that HHS is working on a health care cyber center which I expect we will also address today.

As with our previous hearing on information-sharing analysis centers, I think it=s so important that we look for solutions. But toward that end I also want to make sure that our solutions are measurable, efficient and effective in protecting our nation=s networks and systems. Defending our nation=s health care sector against a wide range of cyber threats requires a coordinated effort involving many players and approaches.

Because this is such an important area, we must continue to find ways to strengthen our cybersecurity systems, particularly relating to health care, including the problem of ransomware and the threat of insurance and medical records theft.

Mr. Chairman, I am looking forward to continuing to work closely on these issues with you as we do our work in this vital area, and I yield back.

Mr. Murphy. Thank you.

I now want to recognize the chairman of the full committee, Mr. Walden.

Mr. Walden. I thank the gentleman for having this very important hearing. This is -- this is really critical work we are all engaged in together.

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

But for all its benefits, the digitization of our daily lives also comes with risk. The internet information technologies are inherently insecure. With time, motivation and resources, someone halfway around the world can find a way into almost any product and system. As the opportunities for attackers proliferate, the potential consequences of their actions are becoming more and more costly and severe. As more product, services and industries become connected to the digital world, we must acknowledge that the threat is no longer just date and information.

It is literally public health and safety. For the health care sector, these factors present a very, 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 target attack on the health care sector, the consequences, as we all know, would 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 cyber security.

For example, the department=s actions in response to

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. The 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 your internal structure as well as outline plans to elevate cybersecurity across the sector.

The sector is operating on borrowed time. Cyberthreat is spreading and left unchecked it will pose an increasingly greater threat to public health. So we appreciate your guidance, your testimony and your leadership on this.

We look forward to continuing the partnership to make sure that Americans are safe and secure wherever they are as it relates to the internet.

With that, I would yield time to the chairman of the Health Subcommittee, Dr. Burgess.

Mr. Burgess. Thank you, Mr. Chairman. I appreciate you yielding. Chairman Murphy, thank you for holding the hearing. It=s a timely topic and, of course, it has real physical consequences.

I am glad to see the recently published Health Care Industry Cybersecurity Task Force Report, which we have now had available. It=s produced by the Health Care Industry Cybersecurity Task Force and it=s a step in the right direction in improving our ability to prevent and respond to cybersecurity events.

It identifies the challenges posed by the health care and public health sector in maintaining security across unique platforms and devices that must work in concert to enable accurate and timely deliverance of patient care.

It=s even more important when we are considering that health care information or health information isn=t something that can be easily changed like a credit card number or a phone number.

The health information that is there is there for life and the integrity of the data is paramount to protecting patient safety.

I can only imagine the consequences of changing a person=s blood type, their allergy list or their disease diagnosis in a system that is relying upon that information to treat patients.

Overall, the health care and public health sector has improved its ability to manage cybersecurity events including the HHS= management of the WannaCry malware.

But the balance between security important data and protecting patient privacy needs continuous evaluation and adjustment. It is indeed a delicate balancing act.

Is there a point where information sharing creates more vulnerability in identifying entities as targets of attack? What happens when a health care organization limits the reporting of breaches of a 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?

So I thank our witnesses for being here. I look forward to these discussions and it should be an eventful morning.

I yield back, Mr. Chairman.

Mr. Murphy. Thank you.

I now recognize Mr. Pallone for an opening statement of five minutes.

Mr. Pallone. Thank you, Mr. Chairman.

This committee has a long history of examining cybersecurity. The federal government continues to make progress towards addressing vulnerabilities in the health care sector. But it=s 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 cyberthreats. More recently, the WannaCry ransomware attack demonstrated that cyberattacks are 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 is making some traction in assisting its own agencies and private stakeholders in confronting cyberthreats.

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 cyberthreats 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 to the health care industry and HHS to consider.

There are no easy solutions for the issues highlighted in this 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 Communication

Integration Center and what challenges it faces in establishing and operating it.

And finally, Mr. Chairman, I am interested in understanding whether HHS has the budgetary resource it needs to appropriately address its cybersecurity responsibilities. This includes efforts to prevent cyberattacks.

It also includes the HHS= responsibilities to hold regulated entities accountable, especially when those entities fail to protect the sensitive health care information that we trust them to safeguard.

And 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 care 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.

And I yield back. Thank you, Mr. Chairman.

Mr. Murphy. Thank you.

And so now I ask unanimous consent that the members= written opening statements be introduced into the record and without objection the documents will be entered into the record.

[The information follows:]

**********INSERT 1**********

Now I=d like to introduce our panel of esteemed federal witnesses for today=s hearing. Mr. Steve Curren, director of the Division of Resilience Office of the Emergency Management Office of the assistant secretary for preparedness in response. Welcome here.

Mr. Leo Scanlon, deputy chief information security officer and designee for cybersecurity for HHS under the Cybersecurity Act of 2015, welcome.

And Mr. Emery Csulak -- did I say that right? Okay. Chief information security officer and senior privacy official, Centers for Medicare and Medicaid Services and co-chair of the Health Care Industry Cybersecurity Task Force.

Thank you all for being here today and providing testimony. We look forward to a very productive discussion on this.

Now, I understand, Mr. Curren, you=ll be the one presenting the initial testimony? But since you all may be asked to comment we will ask you all to be sworn in.

You=re all aware that since this committee is holding an investigative hearing when so doing it has the practice of taking testimony under oath. Do any of you have objections to taking testimony under oath?

Seeing none, the chair then advises you that under the rules of the House and rules of the committee you are entitled to be advised by counsel.

Do any of you desire to be advised by counsel during testimony today? And seeing none there, too. In that case, will you all please rise and raise your right hand. I=ll swear you in.

[Witnesses sworn.]

Thank you very much. Seeing that all have answered in the affirmative you=re now under oath and subject to the penalties set forth in Title 18 Section 1001 of the United States Code.

So members are aware, I mentioned that the department has submitted one written testimony on behalf of all three witnesses. Each plays a distinct cybersecurity role within the department.

They will each -- they will give a brief opening statement describing their roles and responsibilities. Mr. Curren will begin before turning to his colleagues. Each witness= testimony -- excuse me, opening statement is reflected in the department=s written testimony.

Mr. Curren, you are recognized for an opening statement.

STATEMENTS OF 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; LEO SCANLON, DEPUTY CHIEF INFORMATION SECURITY OFFICER, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES; EMERY CSULAK, CHIEF INFORMATION SECURITY OFFICER AND SENIOR PRIVACY OFFICIAL, CENTERS FOR MEDICARE AND MEDICAID SERVICES, CO-CHAIR, HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

STATEMENT OF MR. CURREN

Mr. Curren. Good morning, Chairman Murphy, Ranking Member DeGette and distinguished members of the House Energy and Commerce Subcommittee on Oversight and Investigations.

I am Steve Curren, director of the Division of Resilience within the Office of Emergency Management in the Office of the Assistant Secretary for Preparedness and Response, or ASPR.

Today I will be discussing ASPR=s functions and cybersecurity mission within the Department of Health and Human Services.

ASPR was authorized by the 2006 Pandemic and All-Hazards Preparedness Act and works within HHS with federal, state, tribal, territorial and local partners to protect the public from the health and medical impacts of emergencies and disasters.

ASPR=s responsibility are broad and include overseeing advanced research development and procurement of medical countermeasures leveraging -- leading federal public health and medical response efforts under the national response framework. Serving as the federal lead agency for the health care and public health sector under the National Infrastructure Protection Plan and providing integrated policy and strategic direction under the national health security strategy.

ASPR=s Office of Emergency Management is responsible for many of ASPR=s core preparedness, response and disaster recovery capabilities.

OEM provides communities with the resources necessary to support disaster planning efforts and ensures that the health care system can respond to a wide variety of emergencies.

Within OEM, I am responsible for ASPR=s continuity of operations program which works to ensure the resilience of HHS= systems and programs in the faces of emergencies and disruptions.

I am also responsible for the critical infrastructure protection program which focuses on the security and resilience of private sector health care partners.

ASPR works with all levels of government and the private sector to mitigate risk from all hazards including physical and cyberthreats. Over the past five years, few infrastructure issues have challenged the health sector more than the proliferation of cyberattacks.

Within our modern system of health care, nearly everything is connected through a system of systems including dialysis machines and electronic health records.

Cyber is both a direct and a secondary threat. It could impact everyday patients in health care delivery by locking down access to important medical information and lifesaving equipment.

It can also exacerbate an existing emergency where hospitals and emergency first responders are already working a frantic pace to save lives. It cannot afford to lose access to communications or risk further delays in their response.

Since 2014, the sector has been hit with a wave of large health care information breaches, compromising the personal information of hundreds of millions of individuals. In 2016, we started to see the rise of health care ransomware attacks. In these attacks, computer malware is used to lock up the files of health care organizations while criminals demand payment in exchange for restored access.

These attacks shifted the threat landscape considerably as they no longer threaten just personal information but the ability of health care organizations and thus communities to provide patient care.

When the massive WannaCry ransomware attack hit dozens of hospitals in the United Kingdom just a few weeks ago, ASPR took immediate action to engage broader U.S. health sector and ensure that IT security specialists had the necessary information to protect against, respond to and report intrusions.

This effort included calls with up to 3,100 participants each, daily messages with answers for frequently asked questions, resources from other federal departments and agencies and guidance on how to report attacks.

Beyond specific threats, ASPR and our partners have decided to organize a joint public and private sector working group for cybersecurity to implement national policies such as the National Institute for Standards in Technology in the cybersecurity framework and the National Cyber Incident Response Plan.

We have also benefited from the Cybersecurity Act of 2015 which provided the sector with a structure to drive its continued engagement in cybersecurity.

ASPR led HHS= efforts to establish and support the Health Care Industry Cybersecurity Task Force, which has completed its term and recently delivered its report to Congress.

In closing, HHS= cybersecurity mission is a national response requiring broad collaboration. The department is committed to safe, secure and resilient cyber environment that promotes cybersecurity knowledge, innovation, confidentiality and privacy in collaboration with government, private sector and international partners.

While the cyber realm is ever evolving and presenting new challenges, please be assured that HHS and our partners are moving in the right direction.

[The prepared statement of Mr. Curren follows:]

**********COMMITTEE INSERT **********

Mr. Murphy. All right. Thank you very much.

I will now recognize myself for some opening questions for five minutes. Oh, we are going to hear from the other ones? All right. I am sorry. I didn=t realize how much this was going to go.

Mr. Scanlon.

STATEMENT OF MR. SCANLON

Mr. Scanlon. Thank you.

Good morning, Chairman Murphy, Ranking Member DeGette and members of the subcommittee. I am Leo Scanlon, deputy chief information security officer and the designated senior advisor for health care, public health sector cybersecurity at the Department of Human Services -- Health and Human Services.

I am also the designated senior advisor of health -- public health. I already said that. I will be discussing the agency=s response to CISA, in particular the designation of senior advisor and the establishment of the Health Care cybersecurity Communications Integration Center -- you can say that three times, too -- otherwise known as the HCCIC.

Both of these actions will support enhanced public-private partnerships through regular engagement and outreach to the sector. These actions are consistent with Executive Order 13800 and are a direct response to the Cybersecurity Act of 2015.

These critically important steps 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 of cybersecurity will align and coordinate the 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 to support the HPH sector risk reduction and resilience.

DSA is the chair of the HHS Cybersecurity Working Group, which is the principal forum for coordinating cybersecurity support and response across all HHS operating divisions and staff divisions.

DSA and the CSWG are tasked with the job of establishing a one stop point of access to HHS cybersecurity capabilitiesB a cyber 311 that will allow access to HHS for the entire sector, especially the small and rural provider entities who rarely interact with the federal government and who need sector-specific mitigation strategies, guidance and follow-on assistance in response to cyberattacks.

The HCCIC is designed to be the central location for HPH information sharing and will allow HHS to extend internal threat sharing and analytic capability to our federal partners, law enforcement and intelligence partners, the National Cybersecurity and Communications Integration Center, the NCCIC, and our private sector partners at the NHISAC and other ISALs.

The most important outputs of the HCCIC, though, are products and guidance that are human consumable by entities that do not have the sophisticated technology that supports machine speed reaction to threat indicators.

Smaller entities need information that they can use no matter what their capabilities are. This includes basic cybersecurity guidance, how-to instructions as well as assistance in contacting specialists within HHS and assistance in accessing federal capabilities such as those that are available through the DHS and the NCCIC.

In the recent WannaCry mobilization, HCCIC analysts provided early warning of the potential impact of the attack and HHS responded by putting the secretary=s operation center, the SOC, on alert. This was the first time that a cyberattack was the focus of such a mobilization and HCCIC was able to support ASPR=s interactions with the sector by providing real-time cyber situation awareness, best practices guidance and coordination with US-CERT and the IRT teams at the NCCIC.

Sector calls generated by ASPR reached thousands of health care organizations and providers. One call had more than 3,000 lines open and continued for more than two hours of questions and discussion.

The experiences provided a rich set of lessons learned and has highlighted the disturbing reality that the true state of cybersecurity risk in the sector is under reported by orders of magnitude and the vast majority of the HPH sector is in dire need of cybersecurity assistance.

The SA, the HCCIC and the CSWG have the long-term task of assisting the sector to shift from a compliance-oriented security posture to a dynamic risk management approach.

This means different things at different levels of the sector but one thing is clear. The regulatory mechanisms that served to call attention to the need to protect PHI and PII are fundamentally challenged by the technical capabilities of threat actor who operate at scale and machine speed and who have brought the specter of life-threatening impact from a cyberattack into the operating rooms and ambulances of our providers and first responders.

HHS is prepared to play a leading role in addressing that challenge.

[The prepared statement of Mr. Scanlon follows:]

**********COMMITTEE INSERT**********

STATEMENT OF MR. CSULAK

Mr. Csulak. Thank you.

Chairman Murphy, Ranking Member DeGette and members of the subcommittee, thank you for the opportunity to discuss the work of the department=s Health Care Industry Cybersecurity Task Force.

In addition to my role as the chief information security officer and senior official for privacy at the Centers for Medicare and Medicaid Services, for the last year I served as the government co-chair of the task force.

The Cybersecurity Act of 2015 required the Department of Health and Human Services to convene top subject matter experts from across industry and government to address the growing challenges of cybersecurity attacks targeting health care.

The task force spent a year receiving and reviewing input from experts from inside and outside the health care industry and the general public in order to develop recommendations and action items for a congressional report that was released earlier this month.

I want to thank the 21 task force members including 17 from private sector organizations whose contributions made this report possible based on their passion to improve the sector.

The task force worked diligently to balance the industry and government perspectives. The task force worked diligently to balance the industry and government perspectives.

The task force discussions resulted in the development of six imperatives along with cascading recommendations and action items.

All of these reflect the need for a unified effort among public and private sector organizations of all sizes and across all subsectors to work together to meet an urgent challenge.

They also reflect shared understanding that for the health care industry cybersecurity issues are, at the heart, patient safety issues.

I want to take this opportunity to provide a brief overview of some of the report=s most important recommendations.

These are the steps that can be taken within the industry as well as by the federal government including recommendations for HHS to consider in addressing the cybersecurity challenges facing the sector.

A few key themes emerged from these recommendations. First, the task force identified the need for cybersecurity leadership.

The report outlines the importance of leadership to drive organizational change and ensure adequate visibility across organizations. For HHS cybersecurity leadership focuses on aligning programs to ensure a consistent message and standards across HHS with engagement of industry.

The task force also addresses the need to reduce burden for small and rural providers who may have additional challenges in meeting HHS regulations.

For industry, leadership focuses on communication with executives, driving change and taking a comprehensive look at the threats facing an organization.

Industry need cybersecurity governance models that work for organizations of all sizes and provider types.

Second, the task force report highlights the importance of protecting medical devices and other health IT. Medical devices and electronic health records expand the attack service which can directly impact patient safety.

Some issues raised in the report including taking a total life cycle approach to 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 product end of life.

Third, the task force found that HHS needs to make the discussion, oversight and engagement around cybersecurity clearly and consistently messaged. This includes completing work on a voluntary cybersecurity framework established in the Cybersecurity Act of 2015 and harmonizing regulations and guidance as part of HHS= sector engagement.

By speaking the same language, barriers to education and improvement of the sector will be lowered. It is clear to members of the task force that we must consider the unique needs of small and rural organizations as well as new entrants and innovators.

These organizations can have different and sometimes more acute needs than large organizations who have already invested in cybersecurity and infrastructure. Harmonizing regulations can help to reduce burden on these organizations in particular and thus increase patient safety.

Finally, the task force calls for continuing to strengthen public-private partnerships. In particular, the task force calls for the establishment of an ongoing public-private forum similar to the task force to further the discussions of health care industry cybersecurity as the industry evolves.

Task force members found this engagement with federal partners beneficial to understand our common cybersecurity challenges and concerns.

These efforts will also enable an ongoing conversation and develop strategies to identify resources and incentives that would help to overcome the barriers faced by small and rural organizations.

While much of what we recommend will require hard work, difficult decisions and commitment of resources, we will be encouraging and unified by our shared values as health care industry professionals in our commitment to providing safe high-quality care.

Thank you for the opportunity to share the task force work and I am happy to answer any of your questions.

[The prepared statement of Mr. Csulak follows:]

**********COMMITTEE INSERT**********

Mr. Murphy. I thank all of our panel for your statements.

I want to read the opening sentence here from the task force -- the Health Care Industry Cybersecurity Task Force -- where it says the health care system cannot deliver effective and safe care without deeper digital connectivity.

If the health care system is connected but insecure, this connectivity could betray patient safety, subjecting them to unnecessary risk and forcing them to pay unaffordable personal costs.

So that end, Mr. Curren, want to highlight why this is important? In your opinion, what is at stake when health care information is compromised by a cyber threat? How bad does this get?

Mr. Curren. Thank you very much for the question.

It is an issue that=s very important to us and that we take very seriously because the risk of attacks to the health care infrastructure from cyberattacks really is confidence in the health care system in general and we think that patients should have confidence in the system to provide care, also to provide protection to their information.

You asked about the need to balance two very important concerns. One concern is the use of electronic medical records and other health technologies to advance care, to link information, to provide medical devices that provide excellent care to individuals as well as provide the security to keep those systems and those devices safe and that is the commitment I think that the task force made as we were involved in their discussions was to advance those issues together because really we can=t do one without the other. We need to rely on these technologies. We also need to focus on keeping them safe.

Mr. Murphy. But along these lines is it -- in terms of what could happen here, whether it is like what happened in the United Kingdom -- blocking a system from working entirely so voluntary surgery and others and emergency care was all diverted. But it could also affect things like information about what is in a medical records, medications a person may take and it could also interfere with the functions of a wide range of medical devices. Am I clear on that?

Mr. Curren. There are potential -- there=s always potential for patient safety issues related to cybersecurity incidents and we like to put that into context.

We don=t think the patient should be -- should overweigh the concern of cybersecurity risk when they go seek care. We do believe the benefits of care, the benefits of these devices and these systems greatly outweigh the risks that are there.

However, we do need to take the risks seriously. What I can say is that HHSBwe are set up to respond to both the cyber impacts of these attacks as well as the potential physical impacts, impacts on health care. Through our program ASPR, just to give the WannaCry example as one example, we worked very closely with

Leo=s organization and the HCCIC. They were active in getting the latest information on the threat, analysing it, understanding what the issues were and communicating that to our partners in the health care sector.

Meanwhile, we were working out of the secretary=s operation center and prepared for any type of health care impact that there might have been to provide resources that ASPR has to assist in those responses.

Mr. Murphy. And I appreciate it. I will get to that in a minute and you did play a vital role here. But I=m concerned about that information about the various roles and capability of HHS.

Has it been adequately conveyed to industry yet? And this has got to be partnership -- a public-private partnership. So we are aware you created the HCCIC and to serve as the nexus for cybersecurity efforts.

But to date there has been little public information about this new center to start. So why did HHS decide to establish the HCCIC? Did someone recommend this and is there a reason for this recommendation?

Mr. Curren. Let me start out, then I will hand it to my colleague, Leo Scanlon. We have had a partnership with the private sector for many years in critical infrastructure protection since Homeland Security Presidential Directive 7 in 2003 started these infrastructure partnerships across 16 critical infrastructure sectors.

What has changed in the past several years is the importance of the cyberthreat and HHS is evolving to meet that threat.

So we work very closely with our partners both internal to HHS as well as externally. So, Leo, maybe expand on the HCCIC.

Mr. Scanlon. Yes, sir.

The impulse to establish the HCCIC, continuing on what Steve just pointed out, is really based on the evolution of the way defense against these threats is carried out.

We=ve learned over the past few years that the machine generated information that we now have from our log files and our firewalls and other defensive devices is an enormous firehose of information and ultimately has to be analysed by people -- by analysts who are specialists who can interpret, understand and put context to this information and that=s best carried out in a collective environment where people sit together and can communicate in real time and be in touch with their external organizations and other partners and this is what the NCCIC floor, for example, is all about.

That=s what it does at a national level. It allows different sectors and organizations and intelligence organizations to be present, communicate and share information.

The HCCIC is designed to do that both across the HHS operating divisions to knit together the very formidable capabilities that exist in each of our operation divisions of CMS, CDC, NIH and put them together in real time and then provide real-time links to our partners externally and that=s the fundamental purpose of it.

Mr. Murphy. Who recommended this?

Mr. Scanlon. Recommended, we -- it was our internal decision to take the existing capabilities that we have that were set up in a disparate fashion, unite them in a common place and take this model of threat sharing which has now become an industry standard and apply it to the challenge that we face.

So it was an immediate response in that sense to the CISA Act requirement that we develop the capacity to share threats in real time with the sector.

So that=s the capability that the HCCIC provided and that was the form that we determined was the most efficient and effective way to do that.

Mr. Murphy. Okay. Thank you.

Ms. DeGette, five minutes.

Ms. DeGette. Thank you.

As I mentioned in my opening statement, the WannaCry cyberattack was really a wake-up call. So I want to talk for a minute about what we are doing to prevent and to respond to these types of attacks in the health care sector.

As we heard, HHS is launching the HCCIC, or the Cyber Center, and in your testimony you said that HCCIC was an integral part of ASPR=s coordinated response to the WannaCry incident.

So I just wanted to ask you, Mr. Curren, as you stated and also I noted in my opening the Cyber Center was established to address gaps in cybersecurity and also to help prevent attacks like this WannaCry attack. Is that right?

Mr. Curren. And this would be the HCCIC.

Ms. DeGette. Yes.

Mr. Curren. Yes, and Leo could talk more to that. Within ASPR we coordinate for the WannaCry incident response. Whether it=s a -- it=s a hurricane, tornado or cyber event, we coordinate for the department. But the HCCIC was one capability within that for this cyberattack to coordinate the sharing of cyber information and response.

Ms. DeGette. So how do you think that this will happen? How do you think the Cyber Center can be effective in protecting HHS= health networks and systems? Go ahead, Mr. Scanlon.

Mr. Scanlon. Thank you. Yes. So the value of the HCCIC is evidenced in the way we were able to work in the WannaCry incident.

There=s a broad and very deep communications capability that ASPR has to the sector. We were able to get another component of information gathered through cybersecurity specialists to provide situational awareness, which is the most important thing in a dynamic event.

Fact are very hard to grab when an attack like this is going on. Attribution, who is doing it, what their intentions are and exactly what=s going to happen next all disappears on a fog of activity.

We were attempting at all times to bring the best knowledge that was available across the sector from US-CERT, from the NCCIC, from our sector partners and communicate that out.

That=s a capability that did not exist in a formalized way until we created the HCCIC and the intention of the HCCIC was to support the ASPR capability. They have all-hazards response. So this is a cybersecurity function that we wanted to bring into the all-hazards response capability.

Ms. DeGette. Uh-huh. Now, can you talk -- can you talk about FDA=s information technology systems? Is that something you can talk about?

Mr. Scanlon. I can tell you about what we did to communicate FDA=s and the most important concerns that were raised in the --

Ms. DeGette. Okay. Yes. Well, you know, there was this GAO report last August that said there were major weaknesses in the FDA=s information technology.

So what I was wondering is, number one, why were the FDA=s IT systems allowed to be so plagued with the security issues and, number two, what=s the agency doing about it?

Mr. Scanlon. I think that it would be more appropriate for us to take that back and get back to you with specific. None of us are from the FDA.

Ms. DeGette. Right.

Mr. Scanlon. So it would be not very --

Ms. DeGette. Okay. So you don=t know -- you don=t know the answers to that?

Mr. Scanlon. I couldn=t give you an authoritative answer.

Ms. DeGette. So from the HSS perspective though, you didn=t have very good visibility into what was happening over there. Is that right? At the FDA.

Mr. Scanlon. You=re referring to the GAO audit and the findings of the audit?

Ms. DeGette. Right. Yes.

Mr. Scanlon. This is not in any of our purview, honestly.

Ms. DeGette. Okay. If you can get back to me that would be good because --

Mr. Scanlon. We would be very happy to do that.

Ms. DeGette. -- you know, what we worry about is -- what we really worry about is that cybersecurity attacks they=re going to come throughout all the government. They=re not just going to focus on one agency. And so that=s why we have to really --

Mr. Scanlon. Well, ma=am, I could say to you though that the -- one of the functions of the HCCIC has been to enhance the existing capabilities across our operating divisions, which are formidable and are -- have been very effective in many, many ways.

And so this is where the agency is taking steps constantly to evaluate, assess and improve our cybersecurity capabilities in all of our operating divisions.

Ms. DeGette. Okay. Do you think there=s more we could be doing?

Mr. Scanlon. There=s always more we could be doing.

Ms. DeGette. And what do you need from us to do more?

Mr. Scanlon. I think we need, as always -- I don=t have to say we are always looking for funds to help us support these activities. We --

Ms. DeGette. So if you want funds to support the activities what would be helpful to us is to know what those activities you need additional funding for.

Mr. Scanlon. We could certainly get back to you with specifics.

Ms. DeGette. Great. Okay. Thank, Mr. Chairman. I yield back.

Mr. Murphy. Thank you.

I now recognize the vice chair of the committee, Mr. Griffith, for five minutes.

Mr. Griffith. Thank you very much, Mr. Chairman. Thank you all for being here this morning. I am curious, as Congresswoman DeGette was talking about the FDA and, you know, she=s right. They=re not going to just try one door. They=re going to try all the doors. So I would hope that they would be included.

Maybe you all can help me out. I=m listening to all these initials being thrown around and this is not an area I=m comfortable with. HCCIC versus Health Care in Industry Cybersecurity Task Force that was called upon to be set up as a part of the Cybersecurity Act. What are the differences in those two?

Mr. Scanlon. Yes. So the HCCIC is simply an easy way to say the large mouthful. The HCCIC is an organization within HHS and it is responding to, as I mentioned, the specific -- in specific the recommendations in the CISA Act, which asked the -- the Cybersecurity Information Sharing Act -- which requested the agency or required the agency to establish the ability to do real timesharing of threat indicators with the sector. So that is what the HCCIC does with respect to the CISA Act.

Mr. Griffith. All right. And then the -- any of you all can answer this who feels comfortable with it -- but the Health Care Industry Cybersecurity Task Force that was supposed to be set up, what is -- what is that doing and how often do they meet?

Mr. Csulak. Okay. The Health Care Industry Cybersecurity Task Force, again, was established as part of the Cybersecurity Act of 2015. It had a very segmented period of time.

It was literally by the legislation to only last 12 months. So we completed our work earlier this year and during that time we met at least monthly with both industry as well as the government to, you know, inform and advise the 21 members of the task force in the creation of this report of really looking and analysing the challenges facing health care sector in --

Mr. Griffith. And we appreciate that the report came out. So you=re telling me that you met at least 12 times during the year, maybe some more?

Mr. Csulak. A lot more than 12 but the minimum was 12.

Mr. Griffith. Could you get -- okay. Could you get us a number on how many times you met?

Mr. Csulak. It is actually in the appendices of the report.

Mr. Griffith. In the -- excellent.

Mr. Csulak. You will see every single meeting that we had and who attended it.

Mr. Griffith. All right. I appreciate that.

And can you tell me how the representatives were selected to be on the task force from both the health care sector and from the federal government?

Mr. Csulak. We did an open call of interested individuals for that. I believe Mr. Curren actually arranged the scheduling of all of that but we had over a hundred candidates who were self-nominated or nominated by their organizations.

We formed a joint working group with NIST, DoD, DHS and HHS to look at the candidates and find candidates who represented cyber security practitioners in the field.

We identified four federal -- each agency, each of those four agencies I just mentioned nominated one person to represent the agency and then those representatives along with members on the task force identified 17 of the over a hundred candidates who were interested in the positions who had clear cybersecurity roles as part of their duties, were not just executives but were actual practitioners and would represent various parts of the industry.

If you look at the legislation we needed to represent certain fields. We wanted to look at medical devices. We wanted to look at providers.

There was a range of capabilities that we wanted to deal with so that=s how they were done. We narrowed those down. We made sure that all of those members could be committed for a year and that=s how it started.

Mr. Griffith. Well, I appreciate that. Now, they came out with a number of recommendations and six imperatives and curious what action is now being taken to see that those six imperatives are addressed.

Fortunately, it=s in the stuff that we have and the first one is define and streamline leadership, governance and expectations for the health care industry cybersecurity. What steps do we take now? We=ve got a report. What=s next?

Mr. Csulak. When we look at it, basically the department, HHS, has had representatives throughout the course of this activity supporting the program.

So although I was the government co-chair for the activities, each of those organizations have leadership representatives.

They have membership on the Cybersecurity Working Group established within HHS and, you know, everybody is basically looking at those. And the task force recognizes there=s a lot there, more than we could ever possibly do in one year, and really each of the groups are now stepping back and saying, you know, how do we prioritize these, where do we find the resources for these and that is kind of an ongoing conversation that=s going through the Cybersecurity Working Group.

Mr. Griffith. And as that conversation goes on, as Ms. DeGette said earlier, you all need to let us know what we need to do, whether it=s legislation or otherwise, so that we can assist you in that because making sure that, as you heard from some of the other questions, making sure that our health records are secure and making sure that we don=t have folks who block us from getting to those records or using them for ill purpose is extremely important to all of us.

Thank you, and I yield back.

Mr. Murphy. Thank you.

I now recognize Ms. Castor for five minutes.

Ms. Castor. Thank you, Mr. Chairman, and thank you to all of you for helping to keep Americans= health records safe and secure.

It=s clear the health care sector faces increasing threats from cyberattacks and I=m concerned about the implications for sensitive patient information.

HHS has a large role to play in protecting those records. Mr. Csulak, the Centers for Medicare and Medicaid Services is responsible for the Medicare and Medicaid electronic health records and I understand CMS helps eligible entities adopt and use electronic health records. Is that right?

Mr. Csulak. How do we help them do that? Again, we published some standards that we do when we are working with any organization. You know, the level and engagement, you know, is interpreted to, you know, what=s appropriate for the various programs.

Ms. Castor. So entities that handle electronic health records must comply with federal privacy and security regulations. It=s crucial that companies are held accountable when they fail to protect consumers= private health information. Do you share that view?

Mr. Csulak. Absolutely.

Ms. Castor. And when a cyberattack occurs and private health information is compromised, HHS has the power to investigate. Specifically, the HHS Office for Civil Rights is empowered to investigate how the breach happened and demand changes to that it doesn=t happen again.

Is that correct?

Mr. Csulak. Correct, for privacy breaches under HIPAA.

Ms. Castor. So do you know what is in the president=s proposed budget for the HHS Office of Civil Rights?

Mr. Csulak. I can=t speak outside of CMS and the task force. I don=t know if one of my other speakers could speak to that.

Ms. Castor. Well, that=s okay. I looked it up. The president is proposing a budget cut of more than $6 million to HHS= enforcement of civil rights and health privacy information.

Would these proposed make it more difficult for HHS to take action against entities that fail to safeguard electronic health records?

Mr. Csulak. You know, I think it=s a tough question. Let me answer it from the task force perspective. The task force perspective recognized that this is going to be an ongoing challenge and how do you actually have an oversight role that scales to the size of this industry with so many providers and health care small businesses out there.

You know, can any one organization really scale up to be an oversight body for over a million providers in the United States?

So the task force approach said look, regardless of the money and the resources of OCR -- Office of Civil Rights, as you mentioned -- you know, HHS probably needs to step back and take other -- look at other ideas.

What are some of the other private partnerBprivate-public partnerships that we can look at? Can we look at models like the SEC=s stuff for audit account financing?

How do we bring in other audit models? How do we look at other ways to do this without just relying on a large audit body within the organization.

So the task force approach really looks at saying regardless of the money there how do we leverage the private industry to more effectively, you know, contribute to that knowledge base and to that body of work.

Ms. Castor. But you=d have to say that when you take cops off the beat that=s not helpful in holding companies accountable that have kind of violated their responsibility for privacy records.

I realize you=re not with the HHS Office of Civil Rights but here is the budget justification about the proposed cuts and it says the budget reduction would require decreases in authorized regional investigators which would limit OCR=s capacity to resolve complaints and perform other related agency functions such as investigations and compliance reviews.

So isn=t that the impression you get that cops would be taken off the beat here?

Mr. Csulak. You know, I really can=t say, you know, around the budget formulation for that activity. All I can say is that from the task force perspective there are options out there and we should be exploring those.

Ms. Castor. Well, according to an article from the HIPAA journal it reports that, quote, AThose budget cuts could affect the agency=s HIPAA enforcement activity."

So as we focus on the role of HHS and health care cybersecurity we must not forget the important role that HHS plays in enforcement privacy and security rules.

I would -- I would hope that if the administration is serious about health care cybersecurity it would make sure that it has all the resources necessary for its cybersecurity responsibilities.

Thank you very much. I yield back.

Mr. Murphy. You know, just -- I=m curious. If you had that information from the HIPAA journal and you could share that with me I=d appreciate that. Thank you very much.

Ms. Brooks, you are now recognized for five minutes.

Ms. Brooks. Thank you, Mr. Chairman.

Mr. Curren and Mr. Scanlon, I=m curious what lessons have been learned since the WannaCry attack. What lessons are -- how are you taking the lessons learned and internalizing them within HHS, Mr. Curren, since the WannaCry attack?

Mr. Curren. Yes, I can -- I can mention too and I=m sure we could talk about many that we learned in the WannaCry attack.

We are an emergency response organization in ASPR. We learn lessons from every emergency we respond to and this is no different. We are actually going through an after action process, which we call it, to get information on what we can enhance for the next response.

Two things I think we did that I think worked very well and we want to repeat. One is operating a cybersecurity response as an emergency response that marshalled the resources of the entire department, and the secretary=s leadership in that was instrumental to working this issue out of the secretary=s operation center sitting next to Leo and working calls with thousands of industry participants, getting information from other departments and agencies really was a helpful way to do it.

I think the second is that the public-private partnerships are essential and we can=t just stand them up during emergencies. We say in emergency management that disaster is not the time to exchange business cards and that=s no different for a cyber incident.

We were able to exchange information with partners who trusted us and we trusted them with the information. We don=t want to have to wait to have the final polished version of every piece of information we want to share before we share it. It=s uncomfortable.

But in instances like -- instances like this when time is of the essence, when systems needed to be patched we needed to get information out there immediately and having those trusted partnerships, being open, having a call on the first day with our partners really helped us to establish those relationships and get that information out there.

Ms. Brooks. And before Mr. Scanlon answers, are there any rules or regulations or policies within HHS that are impeding those lessons learned?

Mr. Curren, any -- anyBbefore we go on to Mr. Scanlon, are there any things that are impeding or obstacles to those lessons that you=ve learned?

And with respect to public-private partnerships, that was the reason that in 2003 your office was created, if I recall --

Mr. Curren. Yes.

Ms. Brooks. -- was to create those public-private partnerships across all sectors between government and industry. And so it should just -- it should just be how we operate, shouldn=t it?

Mr. Curren. That is correct, and that is something we=ve been doing for a long time. I think if anything=s evolved in the past several years it=s just the number of organizations involved in cybersecurity that we=ve continued to partner with and we=ve really grown that part of the partnership and that really came into play with WannaCry.

In terms of regulations or challenges that we are going to address, we are working through a number of issues that we think can help enhance the response and some of the matters we are looking at include protections for information and they come into the federal government.

We know the private organizations don=t always look to the federal government as the first place to share and they=re concerned about legal liability with doing so.

Even when we have protections in place it=s essential that we are able to communicate those protections in real time so they can understand them, appreciate them and be compelled to or feel free or feel open to share that information with us.

So that=s something that we need to do because it=s a voluntary mechanism going to the federal government in most cases for this type of sharing.

So the protections that were provided in the Cybersecurity Act I think take us a long way. I think we still have some work to do in terms of implementation and really communicating that to our partners.

Ms. Brooks. Thank you.

Mr. Scanlon.

Mr. Scanlon. The -- to your question as to policies that may impede, our experience in WannaCry was not so much that there were policies inside HHS that impede the communication in this emergency but it was misunderstanding of HHS policies as they=re currently formulated widely through the sector that caused people to have a number of false ideas that we heard on the calls.

For example, many medical device manufacturers and even users of those devices believe that FDA does not allow you to patch a device. This is absolute incorrect. FDA makes great efforts to demystify that problem.

But it is widely believed through the sector. We found that there was a tremendous need to communicate and will be an ongoing need to communicate broadly and deeply what FDA=s policies actually are.

Similarly, with OCR, and to Representative Barton=s questions, there are many beliefs or misunderstandings about what you can and cannot report. But the statute -- PCII, HIPAA and CISA -- are very, very clear in their encouragement of reporting of cybersecurity information during an incident.

And, again, we feel that there=s a need for much better communication. We are undertaking an effort internally to look at how we are presenting these policies to put them into more, if we can, plain language and to provide plain languages guidance that is agreed upon by us and other partners that we can get to the sector, that we can get to the incident response teams and really give them a framework in which they can communicate with us.

Ms. Brooks. Thank you. My time is up. I yield back.

Mr. Murphy. Thank you. I now recognize the gentleman from New York, Mr. Tonko, for five minutes.

Mr. Tonko. Thank you, Mr. Chairman. Thank you and Representative DeGette for this hearing. I think the topic is extremely important.

Cybersecurity is a serious and multifaceted issue that will require an investment of significant resources and you began to get into that with earlier questioning from Representative DeGette.

And I understand that the president=s budget includes some additional funding for cybersecurity efforts at HHS. Mr. Scanlon, how much of this new additional funding would be used to support the new Health Cybersecurity and Communications Integration Center?

Mr. Scanlon. Well, sir, I don=t know exactly the dollar figure of the new funding, what is going -- we are currently -- we have built the HCCIC essentially out of hide. We have taken existing capabilities and investments that have been planned and executed and realigned and repurposed those things to achieve this capacity and then we=ve added in some of our additional technical spending.

But we are anticipating budget increases and proposes to be put into a line item for so that we can get a direct picture of what HCCIC needs and we would be looking forward to give you any more detail that we could about that.

Mr. Tonko. Okay. And also, Mr Scanlon, and I=m asking this question because we want to make certain that our house is in order and that HHS has sufficient resources for its own IT security internally.

The Office of Management and Budget estimates that HHS is pending $13 billion on information technology. During fiscal year 2016, only about $373 million, as I=m informed, or 3 percent of the HHS IT budget, was devoted to IT security.

So my question to you, Mr. Scanlon, is can you give us an updated figure as to how much of the HHS budget for IT is devoted to IT security for fiscal year 2016?

Mr. Scanlon. So I think we could get back to you. The CIO is actively working the budget right now and we=d be glad to get back to you with a detailed picture of the planned and current spending.

Mr. Tonko. Okay. That was fiscal year 2018. I think I might have misspoken and said 2016. So you can get back to us. Can you give me an answer in writing after this hearing?

Mr. Scanlon. Certainly.

Mr. Tonko. And will you give me an answer?

Mr. Scanlon. Yes, sir. I will.

Mr. Tonko. Okay. To make it a little more defined.

Thank you. I=m happy to hear that you will provide us with a response to my question, especially since I=ve been reading reports that a White House lawyer is telling agencies not to answer questions from Democrats. So it=s reassuring.

GAO recently found serious weaknesses in the security computer systems at the Food and Drug Administration. GAO also found that FDA spent only about 2 percent of its IT budget on information security.

Mr. Scanlon, what assurances can you give us that HHS is appropriately prioritizing cybersecurity as part of its overall IT efforts?

Mr. Scanlon. I can tell you, sir, that the FDA response at the GAO audit was robust and vigorous and continues to this day. They have developed what we believe is a world class implementation of a network operating and security operating center to support their ongoing cybersecurity activities.

They are major partners with us in malware analysis. They have one of the strongest groups of malware analysts in the agency and they continue to proceed to respond to that audit and to the generalized threat.

The CIO has in the last year gotten agreement -- this is a milestone agreement for HHS for all CIOs to sign onto a IT strategic plan. It includes an investment plan that places IT security at the center of the strategy for the agency and at the center of the work plans for each of the CIOs.

This was developed collaboratively over a period of time, was signed onto by the CIOs, supported by the CISOs and is being executed and as part of the budget plan of what the agency is doing. The HCCIC itself is another element of a response to further enhance, consolidate and strengthen the ability of the agency to utilize the resources, the strongest -- find the strongest resource that we=ve got in any one OpDiv and make it available as a force multiplier to other operating divisions.

So we are reimagining, if you will, or reorganizing the way we deal with cybersecurity so that we have the strongest and most effective use of the resources that we have.

Mr. Tonko. Thank you. And when will that all be implemented? Is there a target date?

Mr. Scanlon. The IT strategic plan is a continuous process that goes on the course of the strategic planning of the CIOs across the board.

The HCCIC is targeted for what we call initial operating capability the end of this month. That means that we will have our full initial technical capability in place.

We will have our funding understood and we will have messaged -- through our organization we have -- we are now in the process of gathering input from the operating divisions and from senior leadership and that once that message is completed by the end of June we=ll be able to have a much more concrete and documentable picture of where we are.

Mr. Tonko. Right. Well, I thank you and I look forward to hearing from you about the IT budget at HHS and whether HHS is devoting enough resources internally to Cybersecurity. So I thank you again. With that, I yield back.

Mr. Murphy. Thank you.

I now recognize Mr. Collins of New York for five minutes.

Mr. Collins. Thank you, Mr. Chairman. I want to thank the witnesses.

This is a very timely topic we are talking about. Now, one of the more important parts of health care cybersecurity in our conversation is the capabilities of small and medium-sized health care organizations and device manufacturers.

All of you today have briefly touched on the topic in your written testimony and there are recommendations within the task force report that address the concern for small and medium-sized businesses.

The fact of the matter is many of these small health care organizations do not have the resources to address cybersecurity.

Even more problematic, they don=t have the qualified personnel working for them to help them understand what=s even at risk.

So if you could in our limited time, if maybe I could start with Mr. Curren and ask you -- maybe spend a minute and talk about that issue directly as it=s small and medium-sized businesses that struggle to make payroll.

They=re having to make trade-offs each and every day whether it=s R&D, manufacturing and then here=s this cybersecurity and I think the reality is too often it=s a last -- the last thing they=re going to think about and yet, we know -- so if you could maybe discuss briefly your thoughts maybe for a minute or so about that and I=d like the other two also speak to that.

Mr. Curren. Thank you -- thank you very much, and I=m certain we would all agree with that that the small and medium and rural health care organizations really have a critical need for health care cybersecurity information and resources, and the cybersecurity task force, of course, pointed that out.

I think it also provided some good -- some good potential solutions or at least options to look at that maybe Emery can fill in on.

We actually have looked at that within ASPR in terms of our sharing of information with health care organizations. It=s very hard for small health care organizations to process the amount of information that=s out there to know what they need to do to protect their systems.

We put out a planning grant in 2015 to Harris Health System in the Houston area. They took a look at the entire -- their colleagues at the entire health care system, small, medium and large-sized businesses to look at what are the information challenges that are out there and who would we need to reach most.

And one of the findings from that study was that the small and medium organizations, exactly those issues that the task force pointed out, are where we need to focus our efforts.

Based on that, we issued this last year in 2016 a grant to the National Health Information Sharing and Analysis Center, the NHISAC.

That was a competitive grant that they won to help them to increase their information sharing specifically for small and medium-sized organizations that may not have the resources to a be a member of their information sharing organization.

So it=s an issue we continue to look at and that we want to really address.

Mr. Collins. That=s encouraging.

Mr. Scanlon.

Mr. Scanlon. Yes, sir. We -- I=d point to the WannaCry event where during the course of that we at the HCCIC were able to produce -- we called them one-pagers, 101s, to begin to answer questions from the small organizations that were on the phone -- how do I patch, how do I detect, what should I look for, what is the main vector that I should.

So we were able to provide this sort of information in real time to folks who don=t have sophisticated cybersecurity teams to back them up and answer their questions. We look forward to continue to do that in a -- as a series of products.

I would like to just mention we once spoke to an administrator of a hospital in Indian Health Service, a very large -- third largest health care organization in the country, I believe, and very, very underfunded in many ways.

And this administrator said to us, we know their social engineeringBwe are catching the phone calls -- we know they=re phishing usBwe see the emails. We don=t know who they are, what they=re going to do next and what we should do about it.

Those three questions are the questions that HCCIC is committed to answer in conjunction with our partners with the support of our colleagues in ASPR and I think that is exactly what the task force was looking for as well.

Mr. Csulak. Yes. When we looked at the task force, you know, this was clearly seen as a major challenge where cybersecurity is a collateral duty in many of these small and medium-sized organizations.

They=re overwhelmed with information sharing. How do we curate that information and simplify it and make it easier for a smaller number of people to, you know, adopt and embrace.

How do we look at comprehensive education for these organizations? It can=t just be an IT security person in there. We need to educate the patients. We need to educate the clinicians.

We need to, you know, bring this to the boards. How do we -- how do we bring that to a comprehensive thing to make sure we do that.

And the report also talks about how do we take shared services -- how do we look at shared services to kind of offload the burden particularly on these small organizations.

How do we partner with industry, with the NHISAC and High Trust on their initiatives that they=re doing around this challenge of small and medium-sized businesses?

So, you know, it=s kind of -- you know, the task force looked at a comprehensive view and there are many ways and many areas, obviously, that they tried to address in the report.

Mr. Collins. Well, thank you that=s all great. We are all focused on the same thing and the unfortunate fact is small businesses sometimes don=t survive a cybersecurity attack that actually puts them down.

So thank you, Mr. Chairman. My time has expired. I yield back.

Mr. Murphy. Thank you.

I recognize the gentleman from California, Mr. Peters, for five.

Mr. Peters. Thank you very much, Mr. Chairman.

I want to ask some questions about the WannaCry event which crippled 200,000 computers in 150 countries.

What assurances do the current U.S. policies requiring cyber protections provide that weren=t present for medical systems in Europe during that attack and basically how are we doing -- how are we better comparatively and how are we not better comparatively? Can you address that?

Mr. Scanlon. So I think you=re referring to the difference and the disparity between the effect on Europe and the effect on the United States.

Mr. Peters. The practices -- was there something that we are doing better than them because we didn=t get -- or was it just good luck?

Mr. Scanlon. In part, it was probably good luck. There=s continuing analysis -- a great deal of analysis to try to determine exactly what happened and why in the course of that event.

But there was certainly a point in time where the effect of the attack changed. I don=t believe we were spared from any -- from everything we=ve seen in an analytical standpoint we were not spared the spread. We were spared the impact.

Mr. Peters. The impact -- okay. Can you help us distinguish which sort of medical industry cyber systems are most vulnerable to Cybersecurity threats like electronic health records, administrative systems, medical devices or machines, telehealth systems?

Mr. Scanlon. This is a very, very important question. The health care sector is somewhat unique -- not entirely unique but it is particularly sensitive to the phenomena of the internet of things and also the fact that many devices were developed and have been developed not with the intention of being on the internet and when they were put into service, when they were designed it was never intended that they would be able to talk to other devices or be attacked yet they are.

So this represents a major investment problem and it produces another problem that on the normal operating standpoint we can deal with quite easily. We can patch our systems without a great deal of difficulty.

We can roll out automated patches across tens of thousands of machines on a basis. You can=t quite do that in a hospital when you don=t know what the impact of that patch is going to be in an operating room or on a medical device that is unique in the way it=s designed and structured.

So the health care sector has a very different type of vulnerability that requires a lot of thought and a lot of effort to begin to address and this is part of the problem that we saw in the WannaCry event is that the devices that were unpatched were impacted by this in a very severe way and the difficulty of getting those patches to them was very, very profound for the users of the devices.

Mr. Peters. The way you=ve answered that question is more systemic than I asked it. So I=m going to take that as implied that we have to continue to figure out what=s going to be happening?

Mr. Scanlon. Yes, sir.

Mr. Peters. But there=s many, many points of entry now, given these different devices and open source practices and it seems to me that that=s going to be part of HHS= role, I assume, is in corralling this information and spreading best practices?

Mr. Scanlon. Yes, sir. We -- and we did that during WannaCry. We -- and the HCCIC and especially the Cybersecurity Working Group has -- which represents the security practitioners across the agency from FDA, from CMS, from OCR, ONC and elsewhere.

We have an effort and a task to basically get on the road and talk to the sector about what we know and help them understand where they have -- where we have resources that can assist and how to put them in touch with resources that we don=t have.

Mr. Peters. In one sense, it=s more challenging than Britain because Britain=s health system is much more centralized and we have a much more decentralized system.

So can you elaborate on the partnerships and what Congress needs to do to improve that -- make sure that everyone=s engaged?

Mr. Curren. I can say that we are working with our partners to enhance the understanding of this issue, especially at the executive level.

Mr. Peters. Who are you referring to as your partners?

Mr. Curren. The partners would be the -- we have a sector-coordinating council, which is the major trained associations in the health care industry as well as large, medium and small-sized companies. We --

Mr. Peters. Hospitals?

Mr. Curren. Hospitals are part of that but also associations like American Hospital Association, which help us reach out to -- you know, as a force multiplier to their members.

Mr. Peters. Right.

Mr. Curren. So those are the organizations that we are working aggressively with to help spread this message to -- that it=s an important issue, an issue we need investment in in the private sector as well.

Mr. Peters. I=m just taking as a takeaway is that we must be at a very early stage of this because we don=t have a lot of specifics about it.

I do hope that you have the resources that you need, that you are sharing best practices among hospitals. Mr. Scanlon, do you have anything further you wanted to add?

Mr. Scanlon. Yes, sir. I just wanted to emphasize the point that you=re making is that the development of communications in this area is very important to us.

We saw during WannaCry that there=s a lot to be learned and a lot to --

Mr. Peters. In the sense of information sharing?

Mr. Scanlon. Information sharing and also alerting. We discovered that it=s very -- it=s very difficult. The sector, as you noted, is very diverse and very disparate. So there is no one single channel that you can just broadcast out to. We have to find ways to reach down into the smaller organizations.

One of the things that we would, of course, like to ask in your help in the future any advice and assistance you can give us to reach the constituents in your district who need to know this. We are -- we stand ready and would really like to assist in that.

Mr. Peters. Well, my time has expired but I=m sure you=d find everyone on this panel desperate to make sure that you=re getting this information to their districts. So I don=t think that=ll be a problem.

Thank you, Mr. Chairman, for your indulgence.

Mr. Murphy. I now recognize Mr. Costello for five minutes.

Mr. Costello. Thank you, Mr. Chairman.

My question is for all witnesses. It=s a little long. Bear with me.

During our hearing on this topic a few months ago we asked our witnesses whether the fact that many different pieces of HHS are responsible for regulating different pieces of the health care sector causes confusion or duplication for companies trying to remain compliant.

I=d like to read to you what one of the witnesses at that hearing said, because I think it sums it up pretty well. Quote, AWhile many regulations that apply to cybersecurity in health care are well-meaning and individually effective, taken together they can impose a substantial legal and technical burden on health care organizations. These organizations must continually review and interpret multiple regulations, some of which are vague, redundant or both. In addition, organizations must dedicate resources to implement policy directives that may not have a material impact on reducing risks."

This observation was also made in the task force report that just came out. Now that HHS has received this feedback from the industry, a twofold question.

Will there be a review that looks at cybersecurity regulations across the department to make sure that they are aligned? Second, if duplicate, confusing, contradictory or ineffective regulations are discovered, as I imagine they probably already have been discovered, how will the department address them?

Will you look to streamline, supersede or otherwise make workably clear the various regulations so that the issue is addressed?

Mr. Curren. I can start off with some comments related to the high-level implementation of the task force report and be happy to have additions from my colleagues.

The task force report really was a milestone both for industry and for HHS. It really set a marker down to say here are all the things that we can do to improve cybersecurity in this nation.

There are more than 100 imperatives, recommendations and action items in the task force report. About half relate to the government and about half relate to the private sector.

So there=s a lot of work for everyone to do. HHS right now is taking a look at the report and all the recommendations that are there, looking at which recommendations might relate to our current authorities and resources where we have programs available, where we can do good work, which ones may be of interest to our partners where we can work with them to help in implementation and also look at a time frame.

There is so much to do and some have -- many have very long time frames in terms of the action items. So we=ll need to prioritize and sequence how we do things.

I think that for us the regulatory review would certainly be part of that overall look. We do need to go through the whole report though and find out where all the priorities are for HHS and for our partners.

Mr. Csulak. You know, I think as you called out in the report, you know, the task force and two of the task force members who spoke in April highlighted these points is that, you know, harmonization of the regulations is a key piece and a key challenge of that.

I think as we=ve looked even before the task force report was completed, you know, we had already been discussing some of these challenges in the Cybersecurity Working Group in HHS to try to address some of these challenges.

So this has already come up. We are really looking at, you know, the potential negative impacts of regulations and, you know, how can we change this from a negative to a positive.

Why are we punishing people for trying to do the good thing when we should be encouraging them to make improvements and so forth?

So do we have an answer for those right now? No. But I know that, you know, ONC and OCR and the other regulatory bodies within HHS were clearly engaged with the task force activities and the recommendations.

They heard directly from the industry partners where they were having challenges and we are hoping very much so that those will come back through the working group as, you know, solutions and activities in the near future.

Mr. Scanlon. Yes. Echoing what my colleagues have said, we are very well aware of two things. One, the reporting on the impact of these regulations is not what we would like it to be. We don=t know exactly how big, bad or indifferent this impact is. We would like to know that. But we do know that it=s very real and we are taking it very seriously.

The second thing is there=s another part of the answer to the question is that we are engaged in an effort through the discussion about the cybersecurity framework, the NIST risk management approach, and shifting the sector from a cybersecurity focus that is merely based on compliance and which is largely risk avoidance or fine avoidance into an actual dynamic management of the risks and to determine what is needed for them to do that.

So we hope that that effort will help shape this and give us a greater insight into where regulations are impeding the ability of organizations to shift out of a pure compliance mode.

And also the extent to which the type of threat -- the regulations that exist were not really designed to deal with a cyberthreat of the type that affects us and as one of the members pointed out, all these systems are vulnerable.

So it=s very, very hard to avoid under some circumstances the sense that we are victimizing the victim and we very much want to get away from that and move people into an active role in the defense of their systems in conjunction with us.

Mr. Costello. Thank you. I yield back.

Mr. Murphy. I now recognize Dr. Burgess for five minutes.

Mr. Burgess. Thank you, and that=s an excellent place to start, Mr. Scanlon, or really any of you -- the concept of victimizing the victim.

Now, Ms. Castor from Florida talked about the Office of Civil Rights in Department of Health and Human Services. When we had our hearing here several weeks ago in April with the public-private partnerships in the health care sector and, again, as Mr. Costello was bringing up, the dual role of HHS and the regulator as well as the -- being responsible for the sector-specific integrity, it came up that there is, under the Office of Civil Rights under their portal there is a -- what=s called the Wall of Shame. Are you guys familiar with that? Is it helpful?

Mr. Scanlon. Sir, we heard you loud and clear at that hearing and we took that matter back to the secretary. He has taken it very seriously and is working on an effort to address the concerns that you raised. We=d like to get back to you in more detail. The work is not complete but it is underway.

Mr. Burgess. Is that something that can simply be taken care of within the agency?

Mr. Scanlon. Yes, sir.

Mr. Burgess. Or would, perhaps, it be better to have legislation? What concerns me is this thing=s been out there. The first infraction was October of 2009.

Mr. Scanlon. It=s still up there.

Mr. Burgess. A facility in Texas. Yeah, and it=s still up there.

Mr. Scanlon. Yes, sir.

Mr. Burgess. And, I mean, you reach the threshold of 500 charts or whatever affected and you=re up there. I don=t know how that affects someone=s ability to -- I mean, does it -- does it affect their ability to stay in business.

I don=t know what kind of follow-up there=s been done on whether or not access to capital has been limited because they appear on the Office of Civil Rights= Wall of Shame at Department of Health and Human Services. I can just imagine that that is a big deal and, again, we are victimizing the victim again. Why wouldn=t we be helping people rather than continuing to penalize them?

Mr. Scanlon. Sir, we are with you 100 percent and we are -- both what we are doing with the HCCIC to try to reach out to help people understand first how to avoid those. There are things that can be done to avoid the problems that -- and put -- people end up on the wall.

At the same time, I think you asked about legislation. This is a matter to be considered at some point. The threat has changed. The nature of the problem has changed.

Mr. Burgess. Correct.

Mr. Scanlon. There are -- there are certainly matters of due diligence that need to be brought to the attention and need to be publicized and people need to be called to account for those things.

There are the matters where people are being are being attacked by attackers who far overwhelm their capabilities to defend themselves and we need to distinguish between those.

Mr. Burgess. Sure.

Mr. Scanlon. We did that initially. We=ve done that in our -- in our approach to cybersecurity in the federal government.

We=ve adopted the risk management framework where we use a risk assessment approach to evaluate these to determine severity and to apply resources to the most severe problem rather than just shotgun at anything we find.

So we think that this is a model that can be applied. That=s why the task force and others are recommending the adoption of the cybersecurity framework approach and we would like to see that reflected.

We hope to see that reflected in the way that the agency approaches these regulatory matters and we would like to continue talking with you about that as well.

Mr. Burgess. Very well. I haven=t gotten enough in-depth research. I don=t know if the Office of Personnel Management is on your Wall of Shame or not. They were actually involved in a breach a couple of summers ago, as you may recall.

Let me just ask you then on -- and I=ve got a number of questions and I will submit them for the record because I=ve got too much to get through in this context.

But what about the concept of -- we had the ransomware attack. Fortunate in this country that it wasn=t as bad as it could have been.

But aren=t there still a couple of sites that are having ongoing damage from that attack where those -- that malware is continuing to try to lock down their files?

Mr. Scanlon. Yes, sir, and we did a call last week to the sector to talk about that. There=s a peculiar feature of the malware is that the virus itself and its encryption payload are two separate parts of the attack.

The encryption payload is either -- has been defused largely or is being caught in many cases by antivirus and other detection systems.

But the virus may have already been present on a system and even if the system was patched, when it reboots for whatever reason the virus goes into action and the attempt of the virus to activate itself can knock over certain Windows systems and bring them down and crash the device and that=s happening globally.

So there=s an iterative process of discovering which machines are still vulnerable, where the virus is resident, not just patching but then reimaging and rebuilding the machines and that that=s what -- that=s what is happening in the instances that we know about.

That=s basically what=s going on and it=s going to take some time for everybody to get this problem rooted out of their systems because of the virulent nature of it.

Mr. Burgess. And I assume you=ll have ongoing help with that. Good. Let me just be sure I understood you correctly. So we can look forward to being able to take a field trip to HCCIC at the end of June. Is that correct?

Mr. Scanlon. We=d be delighted to have you.

Mr. Burgess. All right. Well, we will -- we will await the invitation. Thank you very much. Thank you, Chairman.

Mr. Murphy. Thank you. I now recognize Mr. Carter for five minutes.

Mr. Carter. Thank you, Mr. Chairman, and thank all of you all for being here. As a health care provider for many years I can tell you this is extremely important and of concern to all health care providers for a number of reasons, not the least of which are the penalties involved with HIPAA and everything else that we are acutely aware of.

Let me ask you, Mr. Csulak -- you=re the co-chair of the Health Care Industry Task Force and that -- that task force has the charge of coordinating industry and the government side to cooperate with and secure digital networks. Is that correct?

Mr. Csulak. Well, we would a task to analyse the challenges and create the report for action. It was, again, a one-year limited version of a task force to come up with these recommendations and is not necessarily and ongoing activity under the current legislation.

Mr. Carter. Okay. Well, can you -- can you describe for me your experiences when you first heard about the WannaCry attack and your interaction with industry? How -- just can you -- can you walk me through that?

Mr. Csulak. Yes. I think, you know, when we looked from a task force perspective on the challenges there, what we really see is, you know, the task force identified and, you know, repeat that, you know, industry and government need to work together about promoting and promulgating best practices in cybersecurity and really, I think when you look at the recommendations that came out of WannaCryВthe action items that came out of WannaCry, they clearly lined up with the task force recommendations of focussing on those best practices, how do we roll those out, making sure that we have good cyber hygiene on our computers.

So, you know, I think the recommendations around WannaCry really do line up and successfully match to the task force recommendations.

Mr. Carter. Can you give me an idea about the quality of the -- of the devices that hospitals are using now? Are they pretty well prepared or the health care facilities, they=ve used a lot of these devices for many years. Are they up to date? Are they prepared? Do we need --

Mr. Csulak. You know, I think -- you know, the task force members really said they run the gamut. You know, we=ve got some organizations which are using state of the art information but there=s a lot of large technology like x-ray machines and other large -- big bill items that really are legacy applications, legacy systems, legacy operating systems which are a challenge.

So I think, you know, when you look at the task force report it looks at some of those challenges. It was, like, look, we need to do a better job developing new stuff. You know, secure operating systems do that.

But we also have to look at architecture and security design issues around how do we segment these systems which are older. We still need to operate on them. Small organizations may not be able to, you know, really easily replace a scanner. How do we help them segment that stuff so it becomes less risky?

Mr. Carter. Do you feel like we are making progress?

Mr. Csulak. I think we are coming -- I think we are making progress. I think if you look at the task force report they really see this as a goal that industry recognizes and can embrace about, you know, coming up with better best practices for this.

So they were very confident that, you know, this is an area where industry really can be a leader in this area and I think, you know, what we are doing is we are seeing progress in there but, obviously, there=s a lot of room to grown.

Mr. Carter. Good. Mr. Scanlon, very quickly -- you=re deputy chief information security office at DHS and the HHS designee for cybersecurity.

One of the things in the cyberthreat preparedness report it identified a number of findings including the fact that there are 11 components within the department that contribute to the health care threat -- the health care sector threat preparedness.

But a consistent concern that we found in preparing for this hearing was that there=s a confusion out there about who to call and, you know, with some of the outside groups.

What are we doing about this to try to clear that up?

Mr. Scanlon. Well, sir, step one -- and we acutely are aware of that internally ourselves. I would like to say, though, on the one hand there is an advantage to this large array of organizations is that we have a 360-degree view of the sector.

So internally our intention is to be able to get that view as a single view that can go out and provide a 311 capability and this is what the Cybersecurity Working Group is primarily tasked with doing.

That is, of course, takes work. That takes time. But we are underway of doing that. We are going to be looking to you for support in that effort as it goes forward.

But that is exactly a problem that we intend to solve and we saw that very clearly in the WannaCry event. We have solid proof of why that needs to be addressed and we think we have a path forward to do it.

Mr. Carter. Great. Well, I=m out of time and I yield back.

Mr. Murphy. Thank you.

I will now recognize Ms. Walters for five minutes.

Ms. Walters. Thank you, Mr. Chairman.

As you mentioned in the testimony, HHS coordinated with NCCIC following the WannaCry attack. I have toured NCCIC and understand the role it plays in the cybersecurity space.

Mr. Scanlon, I=d like to get your thoughts on how the HCCIC fits into the public-private partnership for the health care sector, specifically how it will work with NCCIC and NHISAC. On the surface, it appears that this could create confusion by adding another layer or could be duplicative of these organizations.

Can you elaborate on how the HCCIC will work with the NCCIC and NHISAC?

Mr. Scanlon. Yes. Thank you very much.

Yes, the HCCIC=s function is to be able to reach into what we were just describing as a very diverse and complex sector and to leverage what exists at the NCCIC level.

So the NCCIC has the capability to coordinate across the sectors, across into the intelligence community and at the federal level through law enforcement.

So the HCCIC=s function is to start to provide a communication channel from the sector, especially the smaller and medium-sized organizations that don=t necessarily know about NCCIC or don=t really know how to get to US-CERT or might when they contact their law enforcement -- local law enforcement official might or might not get in touch with some federal level capability.

The HCCIC can leverage what ASPR already has, which is this tremendous ability to reach into the sector and become a vehicle -- a transmission vehicle up to the NCCIC and do something that NCCIC on its own as an organization is really not quite designed to do. It=s got a different function.

Ms. Walters. Right.

Mr. Scanlon. At the same time, the HCCIC is a vehicle to coordinate with private-sector partners. The ISALsBthere are many ISALs. Emery mentioned High Trust as one that=s very active. NHISAC is the grant award organization that is building out a portal that we intend to share with and provide as another major point of contact.

The sector works with many, many channels. Different organizations communicate in different ways. What we are trying to do in the course of this is get out the word that this is where you can get coordinated information and we would like to be able to and intend to be able to reach to each of these partners and work with them and we did do that during the WannaCry event.

We were -- High Trust was on the call. NHISACs were on the calls. They were able to provide insight and information that they had from their activities to the rest of the sector and we would like to make that not just an emergency event but an ongoing activity that the department carries out on a daily basis.

Ms. Walters. Okay. Were these organizations involved in the discussions or decision to establish the HCCIC?

Mr. Scanlon. Not directly. We knew that the grant from ASPR and ONC was going to ask somebody to do that. So we didn=t discuss with any of the bidders or the grant recipients.

But we did discuss among ourselves how we would then be able to respond once that grant was awarded what would the agency do on its side to be able to work with that partner.

Ms. Walters. Okay. So does -- so HHS does not have any discussions with the Department of Homeland Security about the establishment of the HCCIC prior to --

Mr. Scanlon. We had extensive discussions. In fact, it was -- it was people in the Department of Homeland Security who suggested that we move and think in this direct.

We have talked to Department of Homeland Security about developing CONOPS. This is a work in progress now. We have talked with them about what -- the very concerns you raised are concerns for us, obviously.

We don=t want to duplicate. We don=t want to reproduce capabilities that DHS already has. We very much want to leverage their capabilities out to, like, the cyber hygiene program, which is a very scalable and valuable thing for the entire sector, and we want to work with DHS to figure out the actual escalation, communication and integration of these capabilities both on the emergency management side, because that=s another aspect of DHS that=s, again, well established and the cybersecurity side through NCCIC and US-CERT.

Ms. Walters. Okay. A second question I have is a concern that we=ve heard raised with regards to the HCCIC is that information shared with the center might not receive viability protections provided under the Cyber Information Sharing Act of 2015.

Has HHS determined whether or not information shared with HCCIC will receive CISA liability protection?

Mr. Scanlon. Our lawyers have reviewed that and we had ongoing work during the WannaCry to clear that up because that is a widespread believe it is not correct.

There is very, very strong protections and PCII, HIPAA and the CISA that encourage the sharing of indicators and defensive measures and identify what information should not be shared -- PII, PHI, attributable information.

And from our standpoint, we need nothing of that type nor do we even need to know entity information in order to carry out the evaluation in analytic work that we do.

So as I mentioned, we are working with our legal teams and review organizations to develop plain language descriptions of how those protections work and what they would provide to the sector so that we can have that available for people to understand and be clear about it.

Ms. Walters. Okay. Thank you. I=m out of time.

Mr. Murphy. I think that concludes all of our questions for this panel.

I do want to say this. I want to commend you all for the work you did on dealing with the WannaCry threat that occurred.

Granted, it was not as mature or developed as it could have been but it was perhaps a good test run of some of your work. So thank you for that, and it was helpful to hear the lessons learned from this as you moved forward on this.

I want to thank all of you for being here participating in today=s hearing. I remind members they have 10 business days to submit questions for the record.

I would ask that all the witnesses please agree to respond promptly to those questions.

And with that, this committee remains adjourned.

[Whereupon, at 11:53 a.m., the committee was adjourned.]