NEAL R. GROSS & CO., INC.

RPTS MORRISON

HIF094020

CYBERSECURITY IN THE HEALTH CARE SECTOR: STRENGTHENING PUBLIC-PRIVATE PARTNERSHIPS

TUESDAY, APRIL 4, 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.

Present: Representatives Murphy, Griffith, Burgess, Brooks, Collins, Walberg, Walters, Costello, Carter, Walden (ex officio), DeGette, Schakowsky, Clarke, Ruiz, and Pallone (ex officio).

Staff present: Jennifer Barblan, Chief Counsel, Oversight

and Investigations; Elena Brennan, Legislative Clerk, Oversight and Investigations; David DeMarco, IT Staff; Blair Ellis, Digital Coordinator/Press Secretary; Adam Fromm, Director of Outreach and Coalitions; John Ohly, Professional Staff, Oversight & Investigations; Jennifer Sherman, Press Secretary; Hamlin Wade, Special Advisor, External Affairs; Jessica Wilkerson, Professional Staff, Oversight & Investigations; Jeff Carroll, Minority Staff Director; Chris Knauer, Minority Oversight Staff Director; Miles Lichtman, Minority Staff Assistant; Kevin McAloon, Minority Professional Staff Member; Jon Monger, Minority Counsel; Dino Papanastasiou, Minority GAO Detailee; and C. J. Young, Minority Press Secretary.

Mr. Murphy. Good morning and welcome to our Oversight and Investigations hearing on Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships. We are here today to talk about cybersecurity in the health care sector. Strong cybersecurity practices are essential in this industry. This isn't just about protecting data or information, this is about patient safety.

For nearly 2 decades, a cornerstone of the nation's efforts to combat cyber threats have been public-private partnerships designed to facilitate engagement and collaboration between the government and private sector. Over time this model has evolved, but the objective remains the same, the unity of effort between those responsible for protecting the nation and those who own and operate the infrastructure that is critical to that mission.

The focal point of these efforts are 16 critical infrastructure sectors, one of which is the healthcare sector. Each sector is organized around several key institutions: a Sector-Specific Agency, that is SSA; Government Coordinating Council, GCC; Sector Coordinating Council, SCC; and Information Sharing and Analysis Center. I hope you all have that. Each of these institutions plays an important role in ensuring participation, collaboration, and unity of effort of the government and private sector participants within each sector.

Despite a number of efforts to improve this model over the years it has achieved mixed results across the various sectors. Some sectors have succeeded in developing robust support and engagement with both government and industry participants. The gold standard to date has been the financial sector. This sector enjoys a strong collaborative relationship with our government partner, the Department of the Treasury, which is noteworthy because Treasury is also the regulator.

In addition, despite having a very diverse sector, they have succeeded in encouraging support and participation from a wide variety of institutions from small community banks to large multinational financial institutions. This extensive membership has helped the sector to establish the nation's most sophisticated and well-resourced ISAC which improves its value to the entire sector.

Another more recent success story has been the electricity sector. This sector of energy has improved collaboration and engagement both with government partners at the Department of Energy and across private industry through senior executive participation on the Sector Coordinating Council. In addition to elevating the priority for industry partners, it has improved coordination and unity of effort with the government.

Despite the relative success of these and several others,

every sector has unique characteristics and challenges that influence the pace of adoption and engagement in these institutions. What works for one sector may not work for others, and as each sector figures out what works best for their participants, however, the lessons from others should not be overlooked or ignored especially for those sectors that continue to evolve.

What brings us to today's hearing, the healthcare sector focus, this sector has long struggled to coalesce around the public-private partnership model especially with respect to cybersecurity. This may be partially attributable to the fact that cybersecurity is a relatively new challenge for much of this sector. However, as health care becomes increasingly digitized, the need to improve cybersecurity must be a priority.

Gaining the acceptance and support necessary to overcome historical obstacles will not be easy for this sector. To start, health care is an incredibly diverse and complex sector, with a wide range of industries and institutions of various sizes, technological sophistication, and resources. It is also a sector where cybersecurity often becomes conflated with privacy or compliance, complicating the discussion. This, in turn, is exacerbated by the fact that a successful public-private partnership depends on collaboration and trust with HHS, an

understandable challenge given the many participants in this sector who are regulated by various entities within the Department.

These and other challenges are understandable and daunting. If I am a small, rural healthcare institution where cybersecurity falls to one employee who is also responsible for managing IT systems and, well, fixing copiers among other duties, what value do I get for the cost of joining the ISAC or listening to guidance from the sector coordinating council? At present, it is hard to answer that question, especially for those institutions already operating on negative margins.

These challenges, however, must be overcome. The cost of failure for patients, as well as healthcare institutions, is too great. Cybersecurity incidents can result in life or death situations if a medical device is hacked or an attack shuts down a hospital's computer systems. And cybersecurity is a collective responsibility and that is why it is imperative that this sector find a way to come together to find a sustainable path forward.

I look forward to hearing more from our witnesses today about the challenges of this sector and what is needed to bring unity and commitment from all participants. These are the folks working in the trenches, and while the sector has shown signs of progress what we will find out today much work needs to be done.

[The statement of Mr. Murphy follows:]

**********COMMITTEE INSERT 1**********

Mr. Murphy. Now I would like to recognize for 5 minutes, Ms. DeGette of Colorado.

Ms. DeGette. Thank you very much, Mr. Chairman. Every day our infrastructure is under attack by those with malicious intent. We are constantly seeing new headlines about vulnerabilities and cyber attacks against our systems which are becoming more frequent and more sophisticated. Cyber threats are a reality we must face. Information systems connected to the internet are integral to the operation of our economy and our government.

While this interconnection is essential, it also brings vulnerabilities that bring serious challenges. They have affected companies from various industries like retail and banking, and now, as the chairman said, we are seeing increasing vulnerability in the health sector. For example, in 2015, more than 113 million medical records were reportedly compromised in cyber attacks. In one wildly publicized case, a cybersecurity breach at Anthem compromised the personal information of nearly 79 million people.

These attacks are a stark reminder that all industries are vulnerable and neither the private sector nor the government is safe from cyber attacks. I am particularly concerned about these vulnerabilities faced by the healthcare sector as more and more Americans suffer the loss of personally identifiable information

and private medical records.

Defending our nation's healthcare sector against a wide range of cyber threats will require a coordinated effort involving many players and approaches. I am very interested to hear today about the information sharing and analysis center, or ISAC. Several industries have established ISACs to encourage private companies to share information about cyber vulnerabilities and attacks. These ISACs have provided valuable assistance to industry in their efforts to bolster cybersecurity.

Federal agencies also collaborate with these ISACs to facilitate the sharing of important information about cyber threats and incidents. I am so happy to have before us today the new head of the National Health ISAC which is the ISAC that coordinates information sharing among our nation's healthcare industry. The National Health ISAC shares information on vulnerabilities relating to healthcare providers, health IT companies, insurers, medical device manufacturers, and pharmaceutical organizations.

I should note though that the National Health ISAC is a relatively new player. I am still interested though in learning about how it can leverage the experience of ISACs in other industries to assist us in the healthcare sector. I am also interested to hear how the National Health ISAC is helping its

members in the healthcare sector prevent the kind of breaches that we have been seeing.

I look forward to hearing the witnesses' perspectives on what challenges and vulnerabilities we face and what is being done and how we can improve. Alongside that is the question of the appropriate role of government in encouraging and supporting these efforts. Because this is such an important area, I also hope in general we can continue to look for ways to strengthen our cybersecurity systems. Particularly as it relates to health care, I hope we can have more hearings about solutions to the threats that we face, including ransomware, hospital cyber attacks, and the theft of millions of Americans' medical information.

Finally, Mr. Chairman, I want to remind the committee that I along with my fellow committee member Susan Brooks, sitting right over there, sent a letter to the FDA last year asking about cyber vulnerabilities in medical devices. As these devices become more advanced and integrated into our networks they are increasingly vulnerable to dangerous cyber attacks. Because of the urgency of this issue, Mr. Chairman, I hope that we can expand in future hearings how the FDA will address emerging threats to medical devices.

While there is certainly no silver bullet when it comes to

solving cybersecurity threats, I am looking forward to hearing from our witnesses about the role that the National Health ISAC can play. I would like to see us take any steps we can to improve healthcare cybersecurity and this may be a valuable piece of that approach.

Thanks again, Mr. Chairman, for having this hearing. I think this is another bipartisan issue that we can all agree that we need to work together to address and to strengthen the integrity of our medical records. I yield back.

[The statement of Ms. DeGette follows:]

**********COMMITTEE INSERT 2**********

Mr. Murphy. The gentlewoman yields back, and now the chairman of the full committee, Mr. Walden.

The Chairman. I thank the gentleman and I thank our witnesses for your testimony.

We are well aware of the threats posed by our increasingly connected society, but nowhere do these risks hit closer to home than on the very technology we rely upon for our own health care. The threats range from ransomware, breaches of patient data at healthcare organizations, the vulnerabilities of pacemakers and other medical devices. Taken in isolation, these and other threats pose serious challenges to healthcare organizations. Collectively, they demonstrate the breadth, complexity, and unavoidable nature of cyber threats in modern society both now and for the foreseeable future.

You know, as technology becomes increasingly integrated with all levels of our health care, cyber threats pose a challenge to the entire sector. Everyone from the smallest rural hospitals to large providers and device manufacturers face some level of exposure and risk. Breaches, exploits, and vulnerabilities are inevitable realities of modern society even for the most well-resourced and sophisticated organizations.

But this does not mean doom and gloom for everyone with an internet connection. It simply is reality and must serve as the

baseline for any discussion about cybersecurity. We may not be able to stop every attack, but as the threats continue to escalate we must do more to minimize the risk. Improving security is a collective responsibility. When we work together, government and private sector, large companies and small, we can do more to improve security than if we attempt to solve it on our own.

An attack on one organization may be prevented elsewhere if we have the infrastructure and mechanisms necessary to communicate effectively with others across the sector. Further, if an event has widespread or national implications, we need to coordinate an effective and efficient response with unity of effort not confusion over roles and responsibilities. That is why for almost 2 decades the United States has worked to establish public-private partnerships to coordinate security planning and information sharing within and across our 16 critical infrastructure sectors which include health care.

Effective collaboration between government and the private sector is vital to elevating our security posture. These partnerships provide a vital link between those responsible for the safety and security of the nation and those who own and operate the infrastructure critical to those objectives.

To date, these public-private partnerships have experienced mixed results. Some sectors have been more successful than

others in coming together both with private sector and government partners. The healthcare sector in particular has struggled to coalesce around these public-private partnerships for cybersecurity. It is this shared goal and that brings us together today.

This hearing marks the important opportunity to hear from our distinguished panelists about what is necessary to bring the healthcare sector together and continue building momentum in the right direction. Simply put, the cost of inaction is too great. As the threats continue to escalate so do our cybersecurity challenges. We have seen the headlines, we know the attacks will continue, but today is about what improvements can be made so we can be better prepared for the inevitable.

With that Mr. Chairman, unless anybody wants the remainder of my time I would yield it back.

[The statement of The Chairman follows:]

**********COMMITTEE INSERT 3**********

Mr. Murphy. The Chairman yields back. I now recognize the ranking member of the full committee, the gentleman from New Jersey, for 5 minutes.

Mr. Pallone. Thank you, Mr. Chairman, for convening this hearing today.

This committee has a long history of examining cybersecurity and while we have made progress it is clear that we still have a lot of work to do. We continue to see increasingly frequent and severe cyber attacks in both the public and private sectors, and yet our dependence on the internet and interconnected information systems only continues to grow. Faced with these realities we must find ways to bolster our defenses.

And this is especially true in the critical sector of health care. Reports of cyber breaches such as the Anthem case highlight the need for all industry members to come together and find solutions. With the interconnection of health records and now with network-connected medical devices, this problem is becoming more urgent.

While there is no single solution to guarantee that sensitive data will not be compromised, it appears that the Information Sharing and Analysis Centers, ISACs, may play an important role in our overall cyber defense strategy. Other industries have used the ISAC model to encourage private companies to share

information about cyber threats, and today we will hear about similar efforts at the National Health ISAC.

Personal information and medical records are increasingly at risk of cyber attack and therefore it is crucial for members of the healthcare sector to have access to information about threats and vulnerabilities. If the National Health ISAC can leverage and share that information it may be able to help strengthen the cybersecurity of the healthcare community.

I am also interested in hearing about what capabilities the National Health ISAC can offer the health industry and what challenges it faces. I am pleased to welcome Merck which has a major presence in my district and in New Jersey at the hearing today represented by Mr. Terry Rice who is vice president for IT Risk Management at Merck. An effective national strategy for security depends on a close partnership between government and the private sector, so I look forward to hearing the perspectives of Merck, Philips and other companies in the health sector.

We are faced with increasing threats in the healthcare sector and that requires us to continue to identify effective ways to strengthen our cybersecurity. And Mr. Chairman, these problems do not have easy solutions. In order to prevent and defend against a growing number of cyber attacks we will need long-term commitments from many players, and I look forward to hearing from

our witnesses about how the National Health ISAC can enhance our cybersecurity and how this committee can support those efforts.

And unless somebody else wants my time I yield back.

[The statement of Mr. Pallone follows:]

**********COMMITTEE INSERT 4**********

Mr. Murphy. All right, the gentleman yields back and so now let's begin here. 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:]

**********COMMITTEE INSERT 5**********

Mr. Murphy. So now I would like to introduce our panelists of security and privacy experts for today's hearing. First, we welcome Ms. Denise Anderson who serves as president of the National Health Information Sharing and Analysis Center, NH-ISAC, as well as chair of the National Council of Information Sharing and Analysis Centers. Prior to this appointment, Ms. Anderson served as vice president of the Financial Services ISAC.

Next, we welcome Mr. Michael McNeil who serves as the Global Product Security & Services Officer for Philips. In this role, Mr. McNeil is responsible for leading the global product security program for the company and ensuring consistent, repeatable processes that are deployed throughout their products and services in the healthcare market. Mr. McNeil is also here today representing AdvaMed, the Advanced Medical Technology Association, as chair of AdvaMed's cybersecurity working group. Welcome.

And lastly, we would like to welcome Mr. Terry Rice, vice president of IT Risk Management and chief information security officer at Merck. Mr. Rice is also a member of the board of directors for the National Health ISAC.

I want to thank all of our witnesses for providing testimony today and sharing your insights on the current state of public-private partnerships and coordinating with cybersecurity

in the healthcare arena. Now you are all aware that the committee is holding an investigative hearing and when doing so has the practice of taking testimony under oath. Do any of you have any objection to taking testimony under an 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 today's hearing? And seeing none, in that case will you all please rise, raise your right hand, and I will swear you in.

[Witnesses sworn.]

Mr. Murphy. Thank you. You are now duly sworn in and are under oath and subject to the penalties set forth in Title 18 Section 1001 of the United States Code. Let's have you each begin with a 5-minute summary of your written statement and we will begin with you, Ms. Anderson. Make sure your microphone is on and pulled close to you.

STATEMENT OF DENISE ANDERSON, PRESIDENT, NATIONAL HEALTH INFORMATION SHARING AND ANALYSIS CENTER; MICHAEL C. McNEIL, GLOBAL PRODUCT SECURITY & SERVICES OFFICER, PHILIPS, AND CHAIRMAN, CYBERSECURITY WORKING GROUP, ADVAMED; AND, TERENCE M. RICE, VICE PRESIDENT, IT RISK MANAGEMENT & CHIEF INFORMATION SECURITY OFFICER, MERCK & COMPANY, INC.

STATEMENT OF DENISE ANDERSON

Ms. Anderson. Good morning, Chairman Murphy and members of the subcommittee. I want to thank you for this opportunity to address this subcommittee.

ISACs are primarily all-hazard, trusted communities that promote the sharing of timely, actionable, and relevant information and provide forums for sharing around threats, incidents, vulnerabilities, best practices, and mitigation strategies. ISACs gather and disseminate information quickly and efficiently. Numerous incidents have shown that effective information sharing works.

The ISACs collaborate and coordinate on a daily basis through the National Council of ISACs and work with the Sector Coordinating Councils. ISACs also work very closely with various government agencies. In partnership with DHS, several ISACs participate in the National Cybersecurity and Communications

Integration Center, the NCCIC, as well as the National Infrastructure Coordinating Center, the NICC, where they play a vital role in incident response and collaboration.

The NH-ISAC is a global, nonprofit organization and its members represent approximately one-third of the U.S. health and public health GDP. In addition to its many services, the NH-ISAC has a representative on the NCCIC floor and fosters a robust machine-to-machine or automated sharing environment. The NH-ISAC is also engaged in two groundbreaking initiatives. The first is the CyberFit suite of services that allows members to leverage the NH-ISAC community to realize cost savings and efficiencies. The second is the Medical Device Security Information Sharing Council, a forum for manufacturers and hospitals to interact and collaborate in order to advance medical device security and safety.

Under an MOU between the NH-ISAC, the Medical Device Innovation, Safety and Security Consortium, MDISS, and the FDA, a number of initiatives are underway including a program for coordinated medical device vulnerability disclosure and a program for medical device assessments. The highly collaborated partnership with FDA, NH-ISAC, and MDISS, is a great example of how industry and government can come together to address cybersecurity issues.

Today, because of advances in technology and the efficiencies of connecting devices by the internet, the cyber threat surface in health care has ballooned and the threat actors have followed. The stakes are very high. The focus has traditionally been on data and privacy, but if organizations cannot deliver services, as was seen in ransomware attacks recently, or data is manipulated or destroyed, patient lives are at risk.

Congress can help meet this challenge by focusing on four key areas: Education and facilitation of the importance of information sharing. One of the great challenges for the ISAC and all ISACs is the lack of awareness among the owners and operators that the ISACs exist and are a valuable tool. Government should regularly and consistently encourage owner-operators especially at the board and CEO level to join their respective ISACs.

A policy statement that provides explicit guidance to SSAs and their sector constituents to integrate into their cyber risk management and preparedness programs their participation in and collaboration in ISACs is key. Another way to facilitate sharing is providing financial incentives through tax breaks or other means to organizations that join their respective ISACs.

Two, protect information sharing. Recently, the Automotive

ISAC was served a subpoena to furnish all documentation related to communications between the ISAC and one of its members. While the subpoena was quashed, the concern is that if courts were to allow broad sweeps for information and using ISACs as one-stop shops to accomplish it, such actions would effectively kill information sharing. The confidential information shared amongst the members of an ISAC should be protected and not subject to disclosure.

Three, eliminate the confusion with the terms ISAC and ISAO. The February 15th, 2015 executive order called on the formation of Information Sharing and Analysis Organizations, or ISAOs. ISACs were the original ISAOs. However, ISACs are much more than ISAOs. It is absolutely essential that the successful efforts ISACs have established over the years not be disrupted. The EO and prominent coverage of ISAOs has led to much confusion within industry regarding ISACs.

We have seen this clearly in the health sector. When FDA announced the need for manufacturers to participate in an ISAO, confusion ensued. The NH-ISAC is effectively serving as the ISAO, but the FDA guidance by using the term ISAO resulted in a lot of confusion that is still being sorted out. Government needs to call out, recognize, and support the unique role ISACs play and not apply ISAO as a blanket term for information sharing.

Four, establish cybersecurity professionals as SSA liaisons. It has become increasingly apparent that industry needs an experienced government representative at the SSA level who understands cybersecurity issues, threats, vulnerabilities, and impacts, as well as the blended threats between physical and cybersecurity. Having an established, clear go-to lead in this area is imperative.

Thank you. This concludes my testimony and I thank you for the opportunity and I look forward to your questions.

[The prepared statement of Denise Anderson follows:]

**********INSERT 6**********

Mr. Murphy. Thank you. Mr. McNeil, you are recognized for 5 minutes.

STATEMENT OF MICHAEL C. McNEIL

Mr. McNeil. Thank you, Chairman Murphy, Ranking Member DeGette, and members of the committee for the opportunity to testify today.

It is critical to both patient well-being and the medical technology industry that medical devices are safe and that risk, including cybersecurity threats, are appropriately managed. AdvaMed, the world's largest trade association representing medical technology manufacturers and its member companies, including Philips, are committed to a robust cybersecurity framework as part of the development and postmarket management of medical technologies.

Our strategies includes not just staying on top of emerging software-based vulnerabilities and potential external threats while anticipating how they might affect our products and solutions, it also includes collaborating with regulatory agencies, industry partners, and healthcare providers to close security loopholes. This includes participation in the Healthcare Industry Cybersecurity Task Force sponsored by Health and Human Services, HHS.

I'd like to emphasize, one, medical device development and security risk management. Medical device manufacturers must

address cybersecurity throughout the product lifecycle. This includes the design, development, production, distribution, deployment, maintenance, and disposal of devices and associated data. Second, system level security. AdvaMed member companies have developed foundational principles for the management of medical device cybersecurity and believe that medical technology cybersecurity is a shared responsibility among all stakeholders within the healthcare community including manufacturers, hospitals, physicians, and our patients.

Third, we need to have coordinated disclosure. Medical device manufacturers should deploy a coordinated disclosure process that provides a pathway for researchers and others to submit information including potential vulnerabilities. Coordinated disclosure processes should define the responsibilities of both the manufacturers and researchers. Whenever potential vulnerabilities involving a medical device are discovered, findings should first be brought to the attention of the manufacturer and/or the FDA for review, analysis, and possible remediations.

Third, information sharing. The industry should share threat and vulnerability information to assist manufacturers in continuously managing their devices' cybersecurity throughout the product's lifecycle. And then fourth, a consensus around our

standards, regulatory requirements, and education. The development of cybersecurity-related consensus standards and regulations should be accomplished collaboratively among the regulators, medical device manufacturers, independent security experts, academia, and healthcare delivery organizations.

The U.S. Food and Drug Administration, the FDA, should be commended for leadership in medical device cybersecurity. The FDA and its cybersecurity staff have worked closely with the medical technology industry and the broader healthcare ecosystem to ensure medical device cybersecurity is considered and addressed throughout all stages of the product design and use.

AdvaMed and Philips are among the organizations that look forward to continuing to work with Congress and the administration to ensure that the medical technology industry maintains a forward-leaning approach to cybersecurity and the devices that they produce are safe for our patients.

Thank you very much for this opportunity.

[The prepared statement of Michael C. McNeil follows:]

**********INSERT 7**********

Mr. Murphy. Thank you, Mr. McNeil. Mr. Rice, you are recognized for 5 minutes.

STATEMENT OF TERENCE M. RICE

Mr. Rice. Thank you. Chairman Murphy, Ranking Member DeGette, and members of the subcommittee, my name is Terry Rice and I have been involved in healthcare cybersecurity for 15 years. I also participate in a number of public-private partnerships that are working diligently to improve the cybersecurity across the healthcare sector and I appreciate the opportunity to testify on this important matter.

Nowhere is cybersecurity challenge more acute today than in the healthcare industry. In just the last few years, as has already been mentioned, we've seen more than a hundred million health records of American citizens in a couple of well-publicized incidents. We have seen how software vulnerabilities in insulin pumps and pacemakers can be exploited to cause potentially lethal attacks. And we have witnessed entire hospitals in the United States and the U.K. shutting down for multiple days to combat ransomware infections in critical systems.

Unfortunately, I believe these incidents underrepresent the risk we are facing in the industry and I make this statement based on five observations. First, the total number of cybersecurity incidents is significantly underreported due to current disclosure laws. Number two, electronic evidence gathered

through normal security monitoring suggests there are a lot more breaches and incidents than what is currently reported. Three, the healthcare industry consists of many small to midsized businesses that lack the capital and personnel to deal effectively with all but the most basic cybersecurity issues.

Fourth, in our industry, the need for portability of health information to adequately care for patients increases the risk unlike many other sectors. Five, recent advances in healthcare technology along with the proliferation of electronic health records and healthcare applications has opened up a much wider array of cybersecurity risks and exposures. The combination of these observations leads me and many of my peers to believe that the cybersecurity situation in the healthcare industry is far worse than what current reporting indicates.

Neither the private sector nor the government can solve this problem alone. We must work collaboratively and transparently to reduce this risk. As a participant and user of services provided through multiple public-private partnerships identified in my written submission, I feel each provides tremendous value and has become an integral and essential part of the defense of my organization.

We consume intelligence from the NH-ISAC on a 24 by 7 basis to update our defenses, we utilize digital identities from the

SAFE BioPharma Association to protect sensitive data, and we participate in the Sector Coordinating Council meetings to discuss emerging topics in the cybersecurity area.

But I think there's a lot of opportunity to do more and I'll cover five of the observations, or five of the items that I hit in my written testimony.

First, HHS should appoint a senior cybersecurity professional with healthcare sector experience as the primary liaison to industry. Today, there are multiple offices within the Department that have some responsibility for cybersecurity outreach, but none of them have it as their primary task. Furthermore, few organizations have the detailed cybersecurity knowledge and experience to engage with their private industry peers. This new role would be the focal point for all cybersecurity interactions with the private sector and would serve as the government lead on the rest of the opportunities.

Number two, HHS should work with the Sector Coordinating Council and private sector to develop a more comprehensive cybersecurity protection plan for the industry. While the high level cybersecurity plans were captured in the latest iteration of the Healthcare and Public Health Sector Specific Plan dated May 2016, a more thorough and detailed plan should be developed. The current plan is only two pages. Third, HHS and the NH-ISAC

should work with DHS, law enforcement, and the intelligence community to increase the quality of intelligence and the speed with which it is shared to the private industry.

Fourth, HHS and the Sector Coordinating Council, the NH-ISAC, should work with the private sector to schedule and execute tabletop exercises and other simulations to assess the effectiveness of the cybersecurity plan within the healthcare environment. These events would be similar to the Hamilton series of exercises conducted by the Department of Treasury and the financial services sector that led to the creation of capabilities such as the Sheltered Harbor concept that is scheduled to go operational this year.

Fifth and finally, HHS, DHS, and the Sector Coordinating Council should collaborate with global agencies and institutions to share intelligence best practices and emerging concerns. This is a global problem. Thank you.

[The prepared statement of Terence M. Rice follows:]

**********INSERT 8**********

Mr. Murphy. Thank you. I will now recognize myself for 5 minutes of questions. So let's start off in identifying what this is, because this gets into a lot of weeds and pretty technical for us.

So what is the worst case scenario? What happens if these problems aren't fixed? What happens in the healthcare sector with everything from medical devices to medical records to pharmaceuticals, all these things, what problems? I mean what is the problem that emerges here, Ms. Anderson?

Ms. Anderson. I think one of the big problems would be if manipulation of data. So if, for example, if a threat actor went in and said I'm going to, if you have a hundred medical records I'm only going to change two or three of them and you have to figure out which ones were manipulated that could actually have a huge impact on patient care and safety, because if someone were a diabetic, for example, and that was taken from their record, or allergic to a particular medicine that could be, you know, very detrimental.

Mr. Murphy. So that would be someone who just for malicious intent they just wanted to cause problems or they would want to --

Ms. Anderson. Maybe to ransom --

Mr. Murphy. Ransom.

Ms. Anderson. -- ware as well, yeah. So we have seen that as, you know, where people have held things for a ransom, ransomware attacks obviously, or even access to their websites or access to information. So that would be a criminal motivation as well.

Mr. Murphy. Mr. McNeil?

Mr. McNeil. So I would build upon the information that Denise just stated and elaborate that if you do manipulate some of the information at least as it pertains to the medical devices that could lead to patient safety directly with the patient's health in terms of either misinformation that is used in diagnosis and treatment as well as the manipulation of how those devices can function.

Mr. Murphy. So real life and death harm or certainly causing complications in the hospital, expensive difficulties emerge from this if we don't fix this.

Mr. McNeil. Correct.

Mr. Murphy. Mr. Rice, do you have anything to add to that?

Mr. Rice. Sure. The patient safety issue is top of mine, but that also would further break down trust and potentially the adoption of new medical technology which could have ramifications on healthcare delivery. There's also the issue of continuity of service as we've seen with the ransomware issues that have come

up in hospitals and not able to provide critical care. And then, finally, the loss of intellectual property and trade secret information, which could have long lasting economic impacts.

Mr. Murphy. Thank you. We will see if we can take care of the technical problems of our sound system. I apologize for that.

So Ms. Anderson, I understand that NH-ISAC and -- it is being held ransom -- has historically struggled to be effective and a reliable resource for the sector. So based upon your previous experience with the financial sector ISAC, which is often considered to be the gold standard among these organizations, what is necessary for NH-ISAC to succeed and are there any unique aspects of the healthcare sector that are particular challenges for you and your organization?

Ms. Anderson. Absolutely. So, you know, with health care, for example, the smaller, there are many, many smaller organizations that you know, your small physician practices. If you go down the street you'll see a chiropractor's practice, a dentist's office, these are all very vulnerable to cyber attacks or incidents and they are probably the lowest hanging fruit and don't have the cybersecurity practices in place.

So being able to encourage those smaller practices, being able make them cyber savvy, being able to educate them on their staff and why it's important to be aware of cybersecurity and

things that they can do to protect themselves against it is important. With the Financial Services ISAC, we're actually now with the National Health ISAC delivering many of the services if not more that the Financial Services ISAC has been able to do for their members. But they have been able to grow over time and they have a successful community of sharing and that's something that we need to build within the NH-ISAC.

Mr. Murphy. Well, let me ask is that maybe Mr. McNeil and Mr. Rice can weigh in this. So when we talk about the membership involved that information flows two ways. It flows down to the members, the doctor's office, the medical supply companies, the hospital, but it also flows upwards and does that help? Does a membership size affect this?

Mr. Rice. It actually flows also a third direction which is laterally and that actually is the greatest volume today. So when one member of the 200-plus companies that are in the ISAC today see something that is hitting their network, they take the information and rapidly pass it to other individual companies that are members of the ISAC. That allows us to take that information, update our defenses before that same actor is able to attack us almost like a neighborhood watch program.

Mr. Murphy. But with this, and we saw this in the financial sector, many banks were hesitant to share information laterally

because it made them look more vulnerable, it affects their stock, et cetera, et cetera. So is this lateral sharing working out okay, Mr. McNeil?

Mr. McNeil. I believe that the lateral sharing will continue to grow. I think it's still in its infancy, to be quite honest, for our particular industry. I think that we're putting in the appropriate mechanisms, one being the postmarket guidance from the medical device sector with the FDA, so that it affords us much more ability for that sharing as a part of the process of us reporting our vulnerabilities to the government and to our constituents.

Mr. Murphy. Thank you. My time has expired. I recognize Ms. DeGette for 5 minutes.

Ms. DeGette. I have several questions, but I want to ask something that I have been wondering about. We keep talking about vulnerabilities of medical devices, and I am the co-chair of the Diabetes Caucus in Congress so that kind of worries me about the insulin pumps, but there is lots of other kinds of medical devices that can be vulnerable too. And I know that Johnson & Johnson warned customers about a security bug in one of its insulin pumps last fall, and then St. Jude dealt with some vulnerabilities in defibrillators, pacemakers, other medical electronics.

I don't know, Mr. Rice, maybe Mr. McNeil, have we actually

had examples of these pumps being, or these various medical devices actually people taking them over or is it just an identification of a threat? Have we actually had attacks?

Mr. McNeil. So I'll speak first.

Ms. DeGette. Yeah.

Mr. McNeil. There has not been a direct communicated reportable hack of a device. It has been in demonstration that those activities could be taking place. At this point in time we don't --

Ms. DeGette. And is the risk of these attacks an individual or is it a whole class of devices?

Mr. McNeil. So the actual devices and what has been communicated are individual in terms of those attacks that have been demonstrated. But ideally, as you can know, if you have multiple devices that have the same types of vulnerabilities and defects then potentially those same issues would take place.

Ms. DeGette. That is why it is so urgent that we try to --

Mr. McNeil. Correct.

Ms. DeGette. Okay. Ms. Anderson, I wanted to ask you a little bit about the ISACs. The purpose of an ISAC is to help private sector entities share cyber-related threat information with one another; is that right?

Ms. Anderson. That's correct.

Ms. DeGette. And the private sector can get this information from the federal government often from the Department of Homeland Security; is that right?

Ms. Anderson. That's correct.

Ms. DeGette. And the Financial Service ISAC where you used to work it was quite successful in allowing that sector to share threat information involving the banking sector.

Ms. Anderson. Correct.

Ms. DeGette. So turning to the healthcare sector, the risks as we have heard today are getting greater which includes risks on insurance companies, hospitals, medical devices, et cetera. That is what you are looking at right now.

Ms. Anderson. Absolutely.

Ms. DeGette. And so, you know, the National Health ISAC has not been around as long as these other ISACs like the financial services or energy sectors, so I guess given your expertise with financial services what more do you think needs to be done to make the National Health ISAC meet its full potential to serve its members effectively?

Ms. Anderson. So I think that being able to make the constituents within the sector aware of the fact that the ISAC exists and that --

Ms. DeGette. That is usually a fundamental.

Ms. Anderson. Yeah, that's --

Ms. DeGette. Tenet.

Ms. Anderson. -- key, right. You know, and to make sure that they -- then it's a valuable tool that they can use to help protect them, because as Terry mentioned one person's defense is everybody else's offense and that's kind of the concept behind the ISACs. So that is key.

You know, mentioning what I mentioned in my oral testimony and written testimony about maybe tax breaks or incentives to get organizations to join, or any other means by through the SSA or others to encourage those constituents to join the ISAC is a best practice.

Ms. DeGette. Now HHS has provided some funding through cooperative agreements to the National Health ISAC, so it looks like they support the concept of importance. What else can HHS, or what can we do to help achieve these goals that you are talking about?

Ms. Anderson. I think again, you know, being able to build into the NIST Cybersecurity Framework that one of the best practices would be to participate in an information-sharing organization, or ISAC if it's critical infrastructure, is something that should be built into those standards, I believe, and then also being able to encourage those players especially

at the CEO level.

I was recently at a conference of rural hospitals and cybersecurity wasn't even spoken about or even on the radar. So there needs to be a huge education made at the CEO and board level that this is important.

Ms. DeGette. Mr. McNeil, maybe Mr. Rice and then Mr. McNeil, you both sit on the board. Do you have any suggestions what can be done?

Mr. Rice. Definitely. I believe as Denise was saying getting somebody in as the sector coordinating liaison to address at the board level. We have 200 members which is a pretty decent start, but the FS-ISAC has 6,000 members.

Ms. DeGette. Wow.

Mr. Rice. And so we need to reach out a lot more to get all of those entities sharing information. And even if only a small percentage are active sharers, if you've got a base of 6,000 that's a lot more data about attacks that are occurring across the ecosystem than even a small percentage of 200.

One of the other challenges is as more and more attacks take place and more information is shared, you need to have the mechanisms to consume the data in an automated way. Humans cannot process that data. Larger entities have the capital and the wherewithal to be able to put in systems and capabilities to

consume and immediately respond. The small rural hospitals are doing it manually. And so there needs to be a way where we can put in the automated capabilities to allow this sharing to occur more effectively.

Ms. DeGette. Thank you. I am out of time, so I don't know if you want to let Mr. McNeil --

Mr. McNeil. The only addition would be tenfold the growth and the education and the communication. That's what we really need to have at this point.

Ms. DeGette. Thank you.

Mr. Murphy. Thank you. I now turn towards the vice chair of the committee, Mr. Griffith, for 5 minutes.

Mr. Griffith. Thank you very much, Mr. Chair, and I appreciate it. I have got to tell you I really like these hearings where we are learning all kinds of interesting information and where we have to figure out how do we make the system better from our positions in Congress.

So Ms. Anderson, let me ask you. In your testimony you described how the Auto ISAC was recently subpoenaed by an entity looking for all communications between the Auto ISAC and one of its members. While the subpoena was ultimately rejected, you say that the incident itself was troubling. Why was this situation problematic, and if you know can you tell me, because

I know the judge ruled that it was just a phishing expedition, but what were they looking for?

Ms. Anderson. They were looking for any communications between that member and the ISAC, which there were a lot of nuances behind it because actually the ISAC didn't exist when the alleged incident occurred, so they were just kind of throwing spaghetti against the wall. But the concern as I mentioned is that if there is a trend for going after ISACs for a one-stop shop shopping for information that could be detrimental to information sharing.

Mr. Griffith. And I do understand that. What specific protections exist or may be necessary to limit the negative consequences of this type of incident or subpoena?

Ms. Anderson. If there were some way that you know, Congress could help protect that information that gets shared confidentially amongst the members, because as we were talking a little bit earlier with the lateral sharing, trust is a key factor in that. And that's the beauty of the ISACs, they are trusted communities. So being able to protect that trust is absolutely key.

Mr. Griffith. And I tend to agree that there ought to be some level of protection, but then I have also heard testimony and discussions today that make me think that maybe we ought to put some limitation on that. So if we have that communication

limited but we said if there is clear or convincing evidence that would indicate that there may have been malfeasance or intentional tortious action, would you agree with that?

Let me explain that so folks -- I know you all get it. But if we have got a fear that insulin pumps or pacemakers or something else may be vulnerable and researchers share that with the ISAC and ISAC notifies the medical device production company or the company that has made it and they take no action and then there comes harm to some individual, obviously there you have, you know, a knowing and understanding that they are risking people's lives by not taking preventive actions. And I would want that information to be able to be shared after a judge ruled that there was some pretty good evidence that something like that happened. Would you not agree with that?

Ms. Anderson. I would agree to it, with it definitely to some extent. I think the information that gets shared within the ISAC probably would not even fall along those lines --

Mr. Griffith. Okay.

Ms. Anderson. -- because we're sharing malicious IP addresses and we're sharing malware and we're sharing phishing emails and subject lines and things like that. So I believe personally that product liability issues probably will not be a factor in something that would want to be collected.

Mr. Griffith. I guess I was thinking in that direction because there was an indication that some of the information that I saw indicated that there was a device that researchers found a vulnerability and instead of going to the company they went to a hedge fund.

Ms. Anderson. Yes.

Mr. Griffith. I would want them to share that through some mechanism with the company so the company could fix it.

Ms. Anderson. Correct.

Mr. Griffith. And then I would want to protect it up to that point, but then if the company shows in a total disregard for safety chose to ignore that information then I would want that information to be available.

Ms. Anderson. Yes, I would agree with you.

Mr. Griffith. Okay. And if we craft something like that you would be all right with that, but you do think there needs to be something that makes it clear they can't just go on phishing expeditions every day because it makes it expensive for the ISAC and makes it troublesome for the companies who are trying to share info.

Ms. Anderson. Absolutely.

Mr. Griffith. All right, I appreciate that. Mr. McNeil and Mr. Rice, on those situations that I put forward do you all have

any suggestions, comments, advice?

Mr. McNeil. Well, I think the first one is at least with the manufacturers and the researchers with the example you gave, if we are following the postmarket guidance which the FDA has issued it would allow us to have more of that coordinated disclosure. And in the event that that coordinated disclosure does not take the fruit that it should bear, then yes, I would be supportive of what you've stated in terms of appropriate requirements from the government associated with that.

Mr. Griffith. All right. And I should note before Mr. Rice speaks that I believe it was your testimony that said some nice things about the FDA. And oftentimes we are only dealing with problems in this committee so it is nice to hear some good things too.

Mr. McNeil. Thank you.

Mr. Griffith. Mr. Rice?

Mr. Rice. The only other point I would add is that after the computer information sharing act of 2015 that was passed we actually did see an uptick because there was some rudimentary liability protections that were put into that act. So I do believe Congress has a role in helping to foster these sharing communities.

Mr. Griffith. I appreciate that very much and with that Mr.

Chairman, I yield back.

Mr. Murphy. The gentleman yields back. I now recognize Ms. Schakowsky for 5 minutes.

Ms. Schakowsky. Thank you, Mr. Chairman. Seems to me that not only are we faced with cybersecurity threats targeting hospitals, insurance companies, and providers, but also the medical devices we use. And I wanted to quote from a 2017 article in Wired magazine that said, quote, Johnson & Johnson warned customers about a security bug in one of its insulin pumps last fall, and St. Jude has spent months dealing with the fallout of vulnerabilities in some of the company's defibrillators, pacemakers, and other medical electronics. You would think by now medical device companies would have learned something about security reform. Experts warn they haven't, unquote.

The cybersecurity warning pertaining to defibrillators manufactured by St. Jude Medical are particularly concerning to me. Right before these concerns were made public, St. Jude Medical and the FDA issued a voluntary recall for these devices due to premature battery depletion. Many patients including one of my staff were required to undergo surgery to replace the defective device.

And I can't imagine going through that ordeal only to find out that the new device, the new device could be vulnerable to

a cybersecurity attack. Just to say this is a young woman on my staff that has a congenital heart condition and it is a really big deal to have to go through an additional surgery, which by the way St. Jude won't pay for all of it. That is another matter.

So Mr. McNeil, what actions are medical device manufacturers taking to make sure medical devices are secure from cybersecurity threats both before and after they reach the market?

Mr. McNeil. So one of the very first areas that a medical device manufacturer needs to maintain and be the mantra that they think about is patient safety. And when you look at the development and the programs that we put in place, we cannot look at the lifecycle of the development of the solutions as we did in the past and years before when you did not have connected environments and you did not have the access that currently exists with these types of products and solutions that are in our patients and in the marketplace.

So first and foremost, you need to make sure that through your development lifecycle that you are doing the appropriate testing and the risk assessments aligned to that clinical environment and the setting that those products and the solutions would be offered. And you have the continuous rigor within your cybersecurity program around the monitoring and the surveillance to ensure that those particular products are free and as much can

be of any types of vulnerabilities.

Ms. Schakowsky. Well, obviously that is what they should do. But, you know, how do we make sure they do that? And also, Mr. McNeil, how do medical device manufacturers alert customers of a potential security risk to their medical device? What policies and procedures do device manufacturers have in place to ensure consumers' notification is timely and effective?

Mr. McNeil. So again I think, number one, you need to be able to do the appropriate security program and initiatives that are stated. Secondly, as a part of that program communications is one of those utmost areas of focus, communications not only with the actual patients or consumers, but also through the federal drug administration, with the FDA because of their direct oversight and guidance over these manufacturers in terms of the development of their products and solutions.

And I think that if you align within those particular frameworks, it affords us the ability to get that effective communication in a timely manner, you know, throughout the system both with the regulation and with directly to the consumer.

Ms. Schakowsky. Well, I understand the U.S. Food and Drug Administration entered into a Memorandum of Understanding with the National Health ISAC and Medical Device Innovation, Safety and Security Consortium to promote cybersecurity information

sharing for medical devices. In December of 2016, the FDA released final guidance on the postmarket management of cybersecurity and medical devices. And further, a medical device-specific information sharing and analysis organization, the Medical Device Vulnerability Intelligence for Evaluation and Response, has launched a streamlining effort to share the information regarding cybersecurity issues. I wondered if anyone wanted to respond to that. Mr. McNeil?

Mr. McNeil. So as a participant, I participate directly from a Philips perspective. We have been directly communicating and working with the NH-ISAC and the MDISS as well as the collaboration with the FDA, and we also have been working with external researchers within our products and solutions to make sure that we're communicating any identified activities from a vulnerability perspective through that particular initiative with NH-ISAC.

Ms. Schakowsky. I thank you. I yield back.

Mr. Murphy. The gentlelady yields back. I now recognize Dr. Burgess for 5 minutes.

Mr. Burgess. Thank you, Mr. Chairman, and I thank you for having this hearing. This is a timely topic and one that is, I think, important to every member of this subcommittee. In fact, on another subcommittee in the last Congress, I was chair of the

Commerce, Manufacturing, and Trade Subcommittee. We did a lot of work on the ransomware issue and it is one that continues to trouble me as a physician in my former life.

Ms. Anderson, let me just ask you, and Chairman Murphy asked you about the Financial Services Information Sharing and Analysis Center. Are there lessons from the financial side that we could incorporate into the healthcare side? And one of the things that strikes me as you all were talking, on the financial side if someone uses my credit card I will oftentimes get a call even if I give it to my staff member and say go get us a hundred Chick-Fil-As for lunch, I will get a call that says is this really a legitimate purchase.

So that is not necessarily a bad thing. They see unusual activity on a financial transaction online and will call it to your attention. Do we have anything that is analogous in the healthcare sector where anyone is doing any kind of looking at a predictive modeling way of notifying a physician or a patient that there is unusual activity regarding their healthcare transaction?

Ms. Anderson. Well, certainly there are security vendors that offer that service, so they're, you know, what we call managed service providers and they're able to monitor the network traffic that you know, if they are employing those services they're

monitoring that traffic and then alerting them on that.

And we're also looking at some initiatives within NH-ISAC where we'll be able to handle traffic that, network traffic for various members as they participate and be able to alert them on things, anomalies that we may be seeing in their environment.

Mr. Burgess. And yet when we do hearings and we talk about problems in the Medicaid system and the Medicare system, the GAO will report back to us that these are high-risk entities that are at high risk for inappropriate payments. We won't call them fraudulent, but let's just put it in the inappropriate payments category. And is there any way we can improve upon what the GAO has told us for years are high-risk activities, can we improve on those with copying the lessons say from the financial sector?

Ms. Anderson. Oh, I would say so, yes. I mean the banks are able, they've, over time they've been able to develop complex algorithms where they're able to monitor traffic and behavior, you know, so payment behavior and pattern behavior of purchasing. So they've absolutely been able to do that and I think it's applicable to the Medicare and Medicaid systems.

Mr. Burgess. Do you know why we haven't done that yet?

Ms. Anderson. I'm sorry. I do not.

Mr. Burgess. Okay, Mr. Chairman, there is the subject of another hearing. Really, this is for anyone. I guess, Mr.

McNeil, it was in your testimony where you talked about the -- no, I am sorry. Mr. Rice, it was your testimony. Anecdotal evidence suggests there is a lot more cybersecurity incidents than what are currently reported.

You know, I have a newspaper article from a few days ago back home in Texas, where a practice in Austin was struck with a ransomware attack. They looked to me like they had done the right things. They didn't pay any money. They had a back-up system. They wiped their servers. Patient care was perhaps interrupted briefly, but only for a period of 24 hours and they were able to be back up and running pretty quickly.

So it almost sounds like a success story, but then further in the article it talks about now they are on the wall of shame from the Office of Civil Rights in Department of Health and Human Services. And you go to the Office of Civil Rights, Department of Health and Human Rights and look at the wall of shame and there are indeed almost 2,000 entities, I think 1,827.

So and I realize this was set up by a congressional directive in the HITECH Act and we told them to open this portal and it goes back to 2009. But is this really serving a good purpose to be punitive to people who again you read the first part of the article it looks like they did everything correctly.

And I identify another practice actually in my district in

Denton, Texas that apparently they had some computer equipment stolen so that theft has now placed them on the wall of shame I guess in perpetuity. Is that the best way we can go about handling this?

Mr. Rice. I think we need to look at each case based on its own merits. In some cases there may be incidents that were well handled as the example that you pointed out. I think the Defense Industrial Base recently has moved to mandatory disclosure, non-publicly, where there can be incident analysis done to determine what the threat actors were, what actions were taken, were the actions appropriate, much in the manner that the NTSB today investigates airline and other types of traffic safety issues.

I think that would be a way to better understand and get a better baseline of the incidents that are actually happening across the board.

Mr. Burgess. But you can say we have got a problem with people underreporting and yet we clobber them when they do report and we put them on this list that is in perpetuity. I just think, Mr. Chairman, I know I am way over time, but I think probably reasonable for us to re-look.

In fairness, I did not vote for the HITECH Act. It was part of the stimulus bill in 2009, so it would be easy for me to say

it is not my problem. But it is all of our problems and I do think that is something that needs to be fixed. Thank you, Mr. Chairman. I will yield back.

Mr. Murphy. Indeed, yes, good point.

Ms. Clarke, you are recognized for 5 minutes.

Ms. Clarke. I thank you, Mr. Chairman, and I thank our ranking member. I thank our panelists for the expert testimony here this morning.

Mr. Chairman, cybersecurity incidents continue to threaten our critical infrastructure including the healthcare sector. A 2015 Financial Times report on health cybersecurity discussed the Anthem breach that resulted in over 78 million people having personal and medical information compromised. This was a truly troubling revelation.

The report said, quote, Anthem's breach sent a wave of panic through the healthcare industry. It exposed clients' most sensitive and valuable personal information and revealed just how unprepared the health industry was to threats from increasingly sophisticated cyber criminals and from nation-states, end quote.

It is now 2017, and I would hope that we have made strides in preventing this type of breach from occurring at Anthem or any other health sector company. So Mr. McNeil, what actions do private sector companies take to prevent breaches like the one

that impacted Anthem?

Mr. McNeil. I think very often companies need to make sure that they're exercising within their own environment. As Mr. Rice, Terry just stated earlier in his testimony, doing tabletop exercises so that you are exercising the rigors of incidents and activities and measurements. That you also, as I would do in our organization, for example, we have a group of actually security we call the ninjas and my team of testers actually go out and test within our environment.

So if you're not doing and exercising internally what potentially could be happening to your organizations from an external perspective, it's hard to always be able to combat that activity.

Ms. Clarke. So to you, Mr. McNeil, and also Mr. Rice, is there significant variation in the cyber capabilities of companies in the healthcare sector?

Mr. McNeil. Yes, there definitely is a variation of capabilities. Because you have very small to very large organizations, and even within the large organizations that doesn't mean that they have the most adequate and up-to-date cybersecurity hygiene and discipline, it's identifying the fact that you need to have a governance program from the top of whatever size that the organization is down to and throughout the

organization.

Based upon that governance you put in the appropriate acumen around doing the testing, developing your products from a secure perspective, understanding how you are developing the solutions, and then making sure that you're testing and monitoring the threats within your entire environment. But yes, I would say that there's work that needs to be done and attention throughout the ecosystem of the organizations in the health care.

Mr. Rice. I would add that one of the things that has helped tremendously in the last couple of years is the publication of the NIST Cybersecurity Framework. That framework identifies a layered defense concept in which first you identify what are your most critical assets, then you try to prevent bad things from happening. But we realize that even the best protected organizations may have issues. So then you need to detect, respond, and ultimately recover if something really goes bad.

Inside of that cybersecurity framework there are maturity levels that allow organizations to start to assess themselves against those controls, and the latest HIMSS study showed that 61 percent of healthcare companies were in the process of adopting the NIST CSF.

One of the things that Denise mentioned that we're doing within the ISAC is this capability called CyberFit and we are

creating a benchmarking capability to allow members to rate themselves across the sector as well as within the subsector. So a small healthcare provider compared to other healthcare providers versus a large pharmaceutical company, they get a good benchmark as to where they stand.

Ms. Clarke. So let me ask the panel, how can the National Health ISAC help some smaller companies bolster their defenses?

Ms. Anderson. I think, you know, being able to bring them into the fold and share information with them make them aware of even why it's important to engage in cybersecurity practices. I was just talking to someone that ran a medical practice and they were not aware, you know, they were told repeatedly by HR do these things, do these things, but they didn't understand the consequences of the fact of when they didn't do it. And so making people aware of the impacts and potential consequences I think is very important especially in these smaller organizations.

Mr. McNeil. I would agree. As a board member that's one of our major focus areas within NH-ISAC is looking at how we can expand the growth and the breadth of the organizations that are participating. And so we are looking at different tiers in order to make sure that that outreach and that awareness, you know, increases. And again I would say our goal is looking at that tenfold growth which has to happen immediately.

Mr. Rice. Under Denise's leadership we have greatly expanded the capabilities that the ISAC brings to the table. And one of the most recent initiatives just started was to divide up and have each member of the ISAC create portions of a security incident response plan or a security operations plan, and then when that is done to donate that into the public domain or at least into the healthcare sector.

So the small entities that don't have a security officer, they can take that document and start to use it at least as a bare-bones capability to deal with any incidents that they face.

Ms. Clarke. Thank you, Mr. Chairman. I yield back.

Mr. Murphy. Mrs. Brooks, you are recognized for 5 minutes.

Mrs. Brooks. Thank you, Mr. Chairman. I do applaud the work that the industry and federal government have done together to ensure that all potential vulnerabilities for individual medical devices and large cyber threats are addressed.

As my friend and colleague the ranking member, Congressman DeGette, mentioned earlier, I am the vice chair of the diabetes caucus and we did write a letter to the FDA outlining several questions about how the agency is working with the industry to mitigate existing vulnerabilities and prevent emerging threats. However, we are still waiting on response. We sent the FDA, in November, two of the questions that we posed. At this point I

would ask unanimous consent to enter our letter into the record.

Mr. Murphy. Without objection, so ordered.

[The information follows:]

**********COMMITTEE INSERT 9**********

Mrs. Brooks. And with that I would like to ask your experience with respect specifically to the FDA, and so Mr. McNeil and Mr. Rice, how has the FDA specifically been working with medical device manufacturers and other stakeholders to assist them regarding potential vulnerabilities and cyber threats in both premarket and postmarket context? Mr. McNeil?

Mr. McNeil. Yes. I would state that approximately maybe 2-1/2 years ago the fragmented system that we currently have from medical device manufacturers specifically, also looking at health delivery organizations that consume a lot of the product as well as the patients, the researchers' organizations, it was extremely fragmented.

I think that over the past 2-1/2 years, the FDA specifically has conducted workshops and specific outreach in order to make sure that they brought the ecosystem, as we call it, of the stakeholders together. It was the first time that that type of activity has truly taken place where you had all of the participants at the same table and exercising around one common goal.

I think also in addition to that the passing of both the premarket guidance as well as the postmarket guidance also helped accelerate and consolidate direction around activities that need to take place from a medical device manufacturer in the

development of our solutions and the type of requirements that should be included in our submissions in our 510(k) and other documentation also was very helpful, as well as how to manage and communicate from a postmarket perspective specifically around the coordinated disclosure.

There was only a few of us from a company perspective over 2 years ago, Philips being one that exercised the coordinated vulnerability disclosure to work with external researchers, now it is something that we look at as a requirement due to the postmarket guidance. So those are direct examples that I would look at and have appreciated by working with the FDA.

Mrs. Brooks. And Mr. Rice, anything additional you would like to add or could you share with us any further explanation about the postmarket guidance on vulnerabilities that need to be shared with patients and consumers?

Mr. Rice. Since we're not a medical device manufacturer it's probably beyond, it's beyond my ability to be able to really provide any additional comment.

Mrs. Brooks. Can you share though with respect to how the FDA has worked with your sector?

Mr. Rice. Yes. And the outreach that's been done through the NH-ISAC particularly, we conduct semiannual summits to attract members. We generally have somewhere in the neighborhood

of 4- or 500 people, cybersecurity professionals from across the industry attends. The FDA I believe has been at every single one of those presenting, updating, listening, and participating actively in the dialogues and discussions.

Mrs. Brooks. Can you both share -- there seem to be multiple agencies within HHS and I was a bit disturbed quite frankly, Mr. Rice, when you mentioned a two-page strategy. Can you please expand on that? Where did that two-page plan come from, and can you both talk a little bit about the various agencies that you work with within HHS? Mr. Rice?

Mr. Rice. Each of the 16 critical infrastructures in the United States are asked to develop sector-specific plans. The Sector-specific Agencies, government agencies, are the coordinating point for that. So every couple of years the sector will develop and update its plan. Currently, the sector-specific plan which covers everything from pandemic flu to healthcare delivery and natural disasters and a wide array of other risks -- it's about a 50-page document -- there are two pages that are devoted to cybersecurity.

I believe that while the material that's in there is helpful, it needs to be significantly expanded particularly for those small entities that don't have large security teams or security professionals even in their organizations.

Mrs. Brooks. Thank you, my time is up. I yield back.

Mr. Murphy. Thanks. Now Mr. Collins, you are recognized for 5 minutes.

Mr. Collins. Thank you, Mr. Chairman. I want to thank the witnesses today. This is certainly a timely topic. It is one that we are going to continue to have for as long we are here.

And so I guess the question I have as an entrepreneur myself, the problem with a lot of what is going on today it is in the entrepreneurial world that most new medical devices are coming, most changes when kind of electronic medical records, these are startup companies spinning off of a university, spinning off of some research institutions, one- and two-man operations. Their total focus is getting their product funded, getting their product to the market. It is not, they are in total denial of anything related to what we are talking about here today, data breaches, or even in the case of a device somebody being able to access it.

So I guess it begs the question on how to, you know, this is a start, education as you said. Is there a cost to join ISAC and if so, is there any thought -- any time an entrepreneur has cost they are going to look at it and they are probably going to say no versus getting in early, so just kind of curious on that.

Ms. Anderson. So with the medical device manufacturers we actually, through the FDA and the partnership with MDISS as well,

have created MD-VIPER which is a community where we can share responsibly disclosure around medical device security and vulnerabilities, and we'll also be providing is that situation awareness around the various threats that are out there. That's still in development; we've just launched it this year. It will be free to people that sign up to participate.

The ISAC membership is a little bit different, but we've gone a long way. As Michael mentioned earlier, we see it as our mission to help everyone within the sector because a rising tide floats all boats. And so, you know, we've reduced our member fees, so our lowest tier right now is $1,200 which is less than a cup of coffee a day. And --

Mr. Collins. No, it is $1,200.

Ms. Anderson. $1,200 per year.

Mr. Collins. Entrepreneur, it is $1,200.

Ms. Anderson. Yes. But we are also working collaboratively. We share with many organizations, other ISACs as well as government organizations at what we call the TLP white and green levels, so those threats that are possible we get those out there as broadly as we can.

One of the things that we did was actually a great public-private partnership story is we worked together with two other ISACs, the Multi-State ISAC and Financial Services ISAC as

well as FBI, Secret Service, and two providers, Symantec and Palo Alto, and we did a series of ransomware road shows across the country in 14 different cities, free to anybody that showed up, where they could learn about ransomware, why it was important to protect against it, and how they could do that.

Mr. Collins. Well, again what I would say is the earlier you get someone in the better. If it costs anything, that is going to be a problem especially for these entrepreneurial companies. And clearly, some of the bigger corporations understand it and at some point you just do your civic duty and bring those folks alone.

When I was the subcommittee chair on Technology on Small Business we had a hearing, and part of the hearing came out if a small company has a significant data breach 67 percent of the companies are bankrupt within 12 months. That piece of data alone was eye-opening enough to a lot of small businesses because we pushed it out, it is like, you know, that is an oh-my-god moment.

And I just acknowledge that a lot of the products being developed, a lot of the software being developed, the developers would acknowledge that cybersecurity is an issue and then they are doing absolutely nothing about it. That is the reality. Wouldn't you agree, Mr. Rice?

Mr. Rice. Absolutely, and I think education is definitely

one of the areas that needs work. It was just a couple of years ago that there was only one academic institution in the United States that required people graduating with a bachelor of science in computer science to take a course, a single course on cybersecurity. And those stats have improved significantly in the last couple years, but you have lots of individuals that learn how to program and want to go off and join a startup company and have not had any experience or exposure to security education. And that's an area where there's plenty of opportunity for improvements.

Mr. McNeil. Again, the education piece is definitely critical, and as you just stated the earlier in the process that we can bring them to the table obviously the better for all of us.

Mr. Collins. Well, it is going to be a continued issue that we all face and it would be naive to think we can put an end to it. And I certainly agree with Representative Griffith that you can't. If you continue just to punish people on a wall of shame there ought to be some due process to get them off because the next person might not disclose; they might look at that as the death of their company. I wasn't even aware of that. That is thinking in the past. That is not forward-thinking, so maybe that is something Congress could work on.

Thank you, Mr. Chairman. I yield back.

Mr. Murphy. The gentleman yields back. I now recognize Dr. Ruiz for 5 minutes.

Mr. Ruiz. Thank you very much, Mr. Chairman. Our nation's healthcare system has been classified as a critical industry for almost 20 years, but still today we see cybersecurity breaches that expose millions of patient medical records to the highest bidder. The fact is our healthcare system is only just entering the digital age, but we must be able to learn from cyber attacks on other industries and implement the best practices developed to respond to them.

It is critical that the healthcare sector take advantage of the expertise developed in these other sectors to safeguard patient data and the integrity of a hospital system. Imagine if there was a cyber attack during a terrorist attack that took down the 911 system. Imagine during that time they also took down our system to communicate in a wireless form with other members.

Imagine if they go into a large hospital network and change the drug allergy information which leaves doctors blind and nurses blind to administer certain medications that may actually hurt and kill the patient. Imagine if they change the dosages of medications that patients say that they need for the illness that is under their medical record. Imagine if they made little tweaks

here and there which can actually cause harm and kill patients.

So my first question is for Denise. What metric are you using to define success for the National Health ISAC, Ms. Anderson?

Ms. Anderson. So I think one of the key metrics is the membership renewals, so people join the ISAC because they find value in it and so that our renewal level is a hundred percent. We've not had anybody drop in the last year since I've come on board, and we're growing. So, you know, the fact that people are finding value in what we're doing is important.

Also we see it in the comments. We just had some threads shared yesterday actually where members were saying this ISAC is great, I'm seeing this as an extended arm to my threat intelligence team. You know, so it's like they're almost seeing it as part of their organization in helping them do what they do.

Mr. Ruiz. How about in terms if its effectiveness and have there been any data that you are measuring in terms of attempts to enter the system and a decrease more that you have identified and those that you have prevented?

Ms. Anderson. Not at this point in time because a lot of that comes from the members themselves. But we are doing some initiatives where we're looking at deploying sensors onto member networks where that network flow will come into the ISAC and we'll

be able to do some analysis on it.

Mr. Ruiz. Okay.

Ms. Anderson. But we do have case studies where we're seeing information sharing where there have been successes, one recently where we shared with the Multi-State ISAC some stuff that we were seeing in National Health. It was an email that was compromised, an account in a utility in actually California and we were able to stop that attack because of what was shared in the National Health ISAC and then working with our partner in the Multi-State ISAC.

Mr. Ruiz. Thank you. Mr. McNeil, I have heard that there is a healthcare cybersecurity task force and that you are participating in it. Can you explain what it is, how it came to be, and what the task force is working on?

Mr. McNeil. Yes. The task force started approximately 1 year ago with the auspice of an executive order, and based upon that executive order to be able to make recommendations around some of the critical areas within the healthcare industry. One of the communications was for us to take a look at other industries and understand the roads that they have traveled and to be able to leverage that activity in regards to the healthcare industry.

We are right now in the process of finalizing that particular recommendation and it will be submitted. Our anticipated time

frame here is the end of April, beginning of May, to the government.

Mr. Ruiz. That is great. So what is your utopian collaborative model between industry, private, public, and just getting everybody together to work on this? What does that vision look like?

Mr. McNeil. I think that particular vision is for us to make sure that there's the collaboration across the different agencies. I think we made the comment that I am governed as a medical device manufacturer by the FDA which is a part of HHS. We have the OCR which also has privacy and other implications. The hospital organizations are also a, you know, participating stakeholder.

Mr. Ruiz. So basically bringing everybody together.

Mr. McNeil. Right.

Mr. Ruiz. This last question is for you, Ms. Anderson. We have a severe cybersecurity expert shortage in this country. It is absolutely horrendous the need versus the supply that we have. There is a program Cal State University San Bernardino that is training in cybersecurity. What educational pipelines do we need to meet the high demand in our nation for cybersecurity?

Ms. Anderson. Absolutely I think that education system is key to developing staff within the cyber skills area. As Mr. Rice

mentioned, you know, being able to build cybersecurity into actual computer science programs is key. I know there's a number of universities and educational institutions that are starting to work on that and certainly we have ISACs that -- we have a REN-ISAC which is the Research and Education Network devoted to universities, and they also are working with it across the college and university level.

Mr. Ruiz. Thank you very much.

Mr. Murphy. The gentleman's time has expired. Now Mrs. Walters, you are recognized for 5 minutes.

Mrs. Walters. I would like to thank Chairman Murphy for holding this hearing, and the witnesses for their testimony.

We are well aware of the growing cyber threats this nation is facing. No industry is immune to the threat of a cyber attack which is why it is important we examine the ways that public and private sectors can work together to maximize our efforts to combat these attacks. There is no question health records contain an individual's most personal and sensitive information. We can all agree that safeguarding confidential health records is critical.

I would like to get some thoughts on how these efforts might be improved. The first question I have is for the entire panel. HHS is obviously a big organization with a diverse set of

responsibilities and cybersecurity is just one of them. That said, I think we can all agree that cybersecurity in health care is immensely important and should be a priority for all stakeholders.

Are there additional actions or initiatives regarding cybersecurity that HHS could take that you think would benefit the sector? And we will start with you, Ms. Anderson.

Ms. Anderson. In my testimony, one of the things I pointed to was having the SSA recognize the ISAC as a best practice for organizations to join and to share information with each other around the incidents and vulnerabilities and mitigation strategies that they have in their environments, so I think that's definitely one way. Another way is to have a clear go-to person who is a cybersecurity professional with experience in cybersecurity and understands the unique nuances of health care and cyber and the blended threats between physical and cyber.

Mrs. Walters. Okay. Mr. McNeil?

Mr. McNeil. It think also in addition there's an opportunity to improve transparency from medical device manufacturer and some of the processes that are used for the development of our solutions. One would be an example of a software bill of materials which allows the manufacturers to describe what the components are, whether or not that's open

source code or material. But if we can increase that transparency that would also force us to have a greater visibility around what might be potential vulnerabilities in our solutions.

Mrs. Walters. Okay, thank you. Mr. Rice?

Mr. Rice. I would argue that the NIST CIF which is the cybersecurity framework that NIST published and has been adopted by 61 percent of the healthcare industry, if we could actually develop implementation guidelines, the NIST cybersecurity framework tells you what you should do. If we could develop guidelines particularly for those smaller entities that are tailored to the healthcare specific area, I think, would go a long way.

And I'd also like to highlight what Mr. McNeil said with the software bill of materials. My daughter has celiac disease. When I go shopping for foods I look at the nutrition label on the package to see if it contains wheat or any type of gluten and obviously avoid that. Today when I'm purchasing software I don't know what is inside that software. I don't know what the components are and I don't have the ability to select or deselect software based on its ingredients.

Mrs. Walters. Okay, thank you. Now that I have asked you what HHS should be doing I am going to ask the opposite and this is another question for the entire panel. Are there issues

related to cybersecurity that you believe are better left to industry to address and if yes, what are they and why are they better left to industry and if not, why not?

And let's start with Mr. Rice.

Mr. Rice. I think that the understanding of the risks within the sector requires industry knowledge. We are a very diverse sector. So if you look at the payer community they're worried about financial criminals. If you look at the pharmaceuticals they're worried about patient safety and the integrity of information and trade secret data. If you look at the hospitals they're worried about continuity of service and the protection of electronic health records.

So industry is probably best at making those risk decisions as to what is the most effective way to address in each area, but it has to be done in collaboration with the government. Thank you.

Mrs. Walters. Okay, thank you.

Mr. McNeil. Again I would just build upon what Terry just stated in terms of that collaboration. Because of the diverse and the uniqueness of the healthcare industry, we definitely would like to see something aligned from a med-cert perspective. Right now we have a computer, you know, emerging response plan and a cert where we identify based upon the severities of the

vulnerabilities, but it is not developed specifically to the healthcare industry based upon how those devices, products, or solutions are deployed in a clinical setting.

So through that collaboration which has to be both public and private I would want to see a reinforcement of that particular area focus.

Mrs. Walters. Ms. Anderson, do you have anything to add?

Ms. Anderson. Very quickly, I think that information sharing should be encouraged but not mandated, and I think it should come from industry because when you share because you want to share it's different from sharing because you have to share.

Mrs. Walters. Okay. All right, thank you. I am out of time. Thank you.

Mr. Murphy. I now recognize Mr. Costello for 5 minutes.

Mr. Costello. Thank you, Mr. Chairman, for holding this important hearing and thank you to our witnesses today for your insight.

My home state of Pennsylvania is indeed a hub for life sciences and medical device manufacturing. AdvaMed companies alone employ over 22,000 Pennsylvanians with nine member companies located in my congressional district. These companies are as diverse as the patients they serve. Zimmer in Exton which specializes in joint replacements employs approximately 14

individuals, while Teleflex headquartered in nearby Wayne focuses on vascular solutions and has a team nearly 12,000 strong.

The fact remains that despite differences in size, specialty, and scope these companies and all the others in between are prime targets for bad actors seeking to cause harm. We all agree that we must take every reasonable action to ensure these companies that specialize in the safeguarding of life have the resources they need to defend themselves and the patient end users they serve against all kinds of cybersecurity threats.

Ms. Anderson, I would like to ask you, regarding NH-ISAC could you describe some of the barriers to entry that do keep small to midsize companies from becoming members and, additionally, upon identifying those barriers to entry what can we do to mitigate them?

Ms. Anderson. So I think first and foremost is the fact that they don't even know that we exist.

Mr. Costello. Right.

Ms. Anderson. And that we can be a valuable tool, so that's huge. You know, when we are able to reach out to healthcare organizations and they see what we offer, we also are offering now a free trial program where they can be participants within the ISAC and get access to everything that's done over a 6-month period. You know, the renewal rate is very high at that point.

We saw that with FS-ISAC when they did that they had a 90 percent success rate in that.

So people need to find, be even aware that it exists, then they need to see the value so they can join. I think money, you know, obviously money is always a factor, but the fact that we've been able to bring it down to less than a cup of coffee a day and we're also exploring things such as scholarship programs and those type of things, bringing people to our conferences, doing free workshops which we do do, as well as, you know, maybe supplementing membership costs, are something that I think are very key.

Mr. Costello. Thank you. For Mr. McNeil and Mr. Rice I am going to run off a string of questions and take them as you find appropriate. In general, what does your interaction with NH-ISAC look like on a daily basis? Two, could you please describe further how NH-ISAC is structured in such a way as to facilitate information sharing even among industry competitors who may be otherwise disinclined to share sensitive information regarding their organization? Three, what more can be done to help organizations feel confident using NH-ISAC to its full potential? And the catch-all, any additional comments you would like to offer?

Mr. McNeil. So from a daily basis in terms of the interaction that we have within NH-ISAC, we have as Denise stated

there are alerts, so there's direct emails that we receive on a daily basis. We also have the ability to participate in different committees and in different activities that the NH-ISAC provides so that also allows us to have a direct access.

We have the biannual summits that is stated so that is another form of participation. They also have workshops that they conduct and that they've rotated. Specifically in my arena we've had these medical device workshops where myself and other members have been able to participate. Structurally, the NH-ISAC allows us to have a constituency of board members and your board member opportunities go from anywhere from 1-, 2- or 3-year slots that we have in place and as well as just our overall membership.

From a competitive perspective in terms of my discussions there, I think the fact that we become, that the word when we said earlier from a trust perspective when you're able to gain the trust among the members of the NH-ISAC and the trust is there, Terry and I will share information just as much as I will share information with J&J, St. Jude, Medtronic, et cetera that you'd name it.

But in order for us to get to that point we had to be able to participate in the initiatives that I've just described in order to help build that trust among our peer group as an example.

Mr. Rice. As far as the NH-ISAC daily interaction, for me

it's the dozens, sometimes much more than that of emails that come in about member companies that are seeing a phishing attack, seeing a denial of service attack, taking that information and then updating our own defenses.

We also see questions that come in through our list server that can be open-ended, like what are you doing about ransomware? And then member companies will respond back to how they're working and operating, and the NH-ISAC staff will collate all that information and publish it into a document that's easily consumable by the members. And as Mr. McNeil indicated, it's also picking up the phone and knowing that somebody on the other side is dealing with the same issues as you and you can provide advice back and forth on how to handle a situation.

As far as what more needs to be done, I stressed in my testimony the need for global engagement. The FS-ISAC is operating in 38 countries today. Cybersecurity is an international problem, it doesn't know boundaries. And so we should be actively addressing and trying to bring in multinational companies and other entities like Interpol and the European enforcement organizations to also share intelligence information about attacks.

Mr. Costello. Thank you.

Mr. Murphy. Thank you. I now recognize Mr. Carter for 5

minutes.

Mr. Carter. Thank you, Mr. Chairman, and thank all of you for being here today. Gentlemen, in the state of Georgia where I am from, earlier this year Governor Nathan Deal, who is a former member of this committee as a matter of fact, he announced $50 million in funding for a Georgia Cyber Innovation and Training Center at Augusta University in Augusta; very excited about that. This is something that we see as being very progressive and very forward-looking and something that I hope that we are going to be able to bring in private industry and bring in, you know, government to work together on these type of issues.

Do you see this as being the trend to have academia involved like this?

Mr. McNeil. Yes, I definitely believe this is the trend and the participation. Number one, I will be at Augusta University --

Mr. Carter. Yes.

Mr. McNeil. -- to help in the next couple of weeks meeting with the team and going over strategically some of the key initiatives. Philips is in a long-term partner and relationship in order to build that out. We also have worked very closely with other academia and institutions in regards to this space, so I believe that it definitely starts there and you'll see that as

much more of a flourishing opportunity.

Mr. Carter. Great, great.

Mr. Rice. I second the comments. We've sponsored an exercise at NC State recently which brought in universities from around the Southeast to participate in a series of exercises that my staff and other cybersecurity professionals then graded so people would get practical experience in addition to the academic experience. I definitely think that this is one of the many opportunities we have to help address the shortfall in the cybersecurity work force.

Mr. Carter. Great. Mr. McNeil, I want to go back to you. Philips is obviously a key player in this area and in many different industries. But can you share with us just some public-private sector collaboration that has been most successful with your company and with some of the private industry?

Mr. McNeil. I think some of the most successful activities has been, one, working with the NH-ISAC, also working with the MDISS organization again getting the word and the education out there. I think that when you talk about for example NH-ISAC, it traditionally had a strong influx from the pharmaceutical and the insurance industries. And due to a number of the cybersecurity activities that the medical device manufacturers are seeing, it now provides us with that type of public-private community in

terms of participation.

I think also when I look at the activities specifically that we're doing, it has afforded us that ability to increase our ability to grow from an information sharing as well as to coordinated disclosures around the researchers. I think also the partnership and the participation with the MDISS organization has reached out directly with the manufacturers and the researcher community. So there were researchers that had not originally been addressed or brought to the table that now are there.

And then, finally, the work with the FDA. From the FDA's perspective and their outreach with their post and premarket guidance as well as a number of the workshops that they've hosted, they have been the catalyst to truly bring the entire ecosystem together and work on issues.

Mr. Carter. Great. Mr. Rice, I want to ask you and I would be remiss if I didn't point out my professional career I have been a pharmacist so I am particularly interested in the pharmaceutical industry and how cybersecurity really impacts you. And I would suspect, you know, in the practice of pharmacy we have HIPAA regulations so we pay particular attention to cybersecurity. That is very important to us.

What about in the pharmaceutical industry? I suspect that with research and development this is critical for your industry.

Mr. Rice. Yes. That is one area of concern within the pharmaceutical industry, and as you're probably aware the healthcare sector outside of DOD is one of the largest, if not the largest investor in research and development and that includes both the government as well as the private sector. So research and development is one aspect. Information about mergers and acquisitions prior to public disclosure, we saw in the FIN4 report from FireEye, a security research company, that there had actually been attacks. Not against the large companies but the smaller companies that were likely to be acquired, these actors would get in and they would be able to get information about which they could potentially trade on.

The second area would be around manufacturing. We run industrial control systems, SCADA systems that automate the manufacturing line, so potential disruptions of that equipment would also cause significant harm. And then finally, being able to disclose financial statements, the integrity of information, the integrity of information in the clinical trial processes that we have, all of those are areas of concern. So it's across almost every aspect of the industry that we see challenges.

Mr. Carter. Great, thank you. And thank you all again for being here and I yield back, Mr. Chairman.

Mr. Murphy. Thank you. Thank you. So in conclusion, I

want to thank all the witnesses and members that participated in today's hearing. This is a pretty difficult subject but something that we have to continue to pursue, as we heard the complex testimony. And I am learning quite a bit myself especially about these acronyms which are your daily breakfast, but as we go through this certainly what we have to pursue is ways of simplifying and making sure that all these different departments work together, especially given what you opened up with what the threats that are out there for life and functions within the hospital and healthcare system.

So again, I thank all the witnesses for participating today. I will remind all members they have 10 business days to submit questions for the record. I ask all witnesses to agree to respond promptly to the questions. With that, this hearing is adjourned.

[Whereupon, at 11:47 a.m., the subcommittee was adjourned.]