To: The Honorable Tim Murphy
From: Mr. Michael C. McNeil
Global Product Security Services Officer
Philips Healthcare
on behalf of AdvaMed, the Advanced Medical Technology Association
Subject: Responses to Additional Questions for the Record
Re: Subcommittee on Oversight and Investigations hearing on
Tuesday, April 4, 2017
Entitled "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships."
Via: Elena Brennan
Legislative Clerk
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Murphy:

This letter is in response to your correspondence of April 27, 2017 addressed to myself on behalf of AdvaMed, the Advanced Medical Technology Association concerning my testimony before the Subcommittee on Oversight and Investigations on Tuesday, April 4, 2017, at the hearing entitled "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships." Cybersecurity vulnerabilities and threats are a persistent, significant and very real threat to many critical American industries. Philips shares your deep concern for and takes very seriously the risks to patients and infrastructure from those who would seek to exploit vulnerabilities in our sector. Philips and AdvaMed are committed to continuing to innovate and implement long-term strategic and effective measures to strengthen our public and private partnerships. We look forward to continuing this vitally important conversation, in order to help meet our goal of improving billions of lives worldwide.

Sincerely,

Mr. Michael C McNeil
Global Product Security Services Officer
Philips Healthcare

Responses to Questions for the Record

The Honorable Tim Murphy
Question 1: I understand that HHS, apparently at the request of DHS, is establishing a Cybersecurity Communications and Integration Center specific to the health care sector, the "HCCIC." It would appear that this organization, at least on some level, replicates the role of an ISAC in other sectors.

Answer: We understand the effort to stand up the HCCIC is underway. AdvaMed member organizations understand and appreciate that cybersecurity is everyone's responsibility, and that it is in this power of shared responsibility and cooperation that we have the best opportunity to protect patients and the greater health care system. Philips is proud of our collaboration with AdvaMed members and the Health care Sector and is very supportive of HHS and the FDA's focus on increasing cyber resiliency.

We are not adequately informed to provide comment on how other sector ISACs are organized as they relate to HHS's planning.

a. What is your understanding of this effort and how does it relate to your organization?

   Answer: We understand that the Department of Health and Human Services is planning to launch the Health Care Cybersecurity & Communications Integration Center by June, as shared by HHS Chief Information Security Officer Chris Wlaschin during an ACT-IAC Mobile Health Forum panel in Washington on April 20. According to news reports, the center will educate health care organizations and patients about the risks associated with using mobile data and applications. The center will be modeled after the Homeland Security Department's NCCIC -- but with a focus on health care – and is scheduled to be operationally capable by June.[1]

   Our hope is that this entity will provide an opportunity to consolidate critical stakeholders for better alignment.

b. Based on your experience, are there other sectors that have their own CCIC?

   Answer: No. I am unaware of other CCICs being stood up beyond HHS and DHS at this time. However, that does not mean it has not happened, it is just not part of my experience. Recent media reports indicate the Centers for Medicare and Medicaid Services are also considering a similar concept according to Mark Scrimshire, a CMS entrepreneur in residence as told to Federal News Radio.[2]

c. Do you think this will be beneficial in addressing some of the challenges in the health care sector?

---

[1] Health care IT News - http://www.health careitnews.com/news/hhs-cybersecurity-center-help-health care-orgs-fight-cyberthreats

[2] Federal News Radio - https://federalnewsradio.com/health-it/2017/04/hhs-to-stand-up-its-own-version-of-the-nccic-for-health/

Answer: Health care networks, like other critical infrastructures, are under persistent attack by bad actors and Philips welcomes new countermeasures and approaches to increase our resiliency across the sector. We understand from reports that HHS sees this kind of collaborative partnership as a logical step, as about 50 percent of U.S. health care organizations lack the adequate tools to deter and manage cyber breaches, according to a 2016 Ponemon Institute study. And as mobile health apps become more prevalent, the department also sees the HCCIC as an opportunity to work with developers to help them more securely safeguard patient data.[3]

d. Are there any potential downsides to having an "HCCIC?" If so, what are they?

Answer: As global threats to our critical infrastructures increase at an exponential rate its wise for HHS and the Health care sector to take innovative, bold approaches to protect our patients from bad actors. Everyday health care is becoming more integrated and interconnected, and we have a mutual responsibility to keep those systems safe. We want to continue to focus on entities such as the HCCIC that bring multiple stakeholders in the ecosystem (health delivery organizations, medical device manufacturers, pharmaceutical companies, researchers, government entities, etc.) together. This can only result in stronger collaboration and trust.

Question 2: According to the membership roster, your organization is a member of the Health care and Public Health Sector Coordinating Council. We know the Health care SCC has many roles and responsibilities beyond cybersecurity, but as cybersecurity becomes more important across the industry, the SCC will arguably have a big role to play.

Answer: You are correct, Advanced Medical Technology Association is in-fact a member of the Health care SCC. The association believes patient safety is the number one priority of the medical technology industry, and member manufacturers are committed to having in place numerous safeguards to ensure the security and integrity of their devices. The ubiquity of digital technologies offers patients significant benefits, and the risk of a malicious cyber-attack is low when compared to these benefits. At the same time, manufacturers recognize the need for increased security with these devices, which is why we are invested in the success of organizations like the Health care SCC.

a. What services, products or value does the SCC offer regarding cybersecurity?

Answer: As detailed in the May 2016 Health care and Public Health Sector Specific Plan (SSP) - since 2010, the HPH Sector partners in the public and private sectors have taken significant steps to reduce sector risk, improve coordination, and strengthen security and resilience capabilities:

- Both the SCC and GCC undertook extensive outreach programs. State, local, and private sector partners were recruited through presentations, webinars, and outreach to national associations.

- The Homeland Security Information Network portal for the HPH Sector was expanded to better meet the information sharing needs of the Sector including a lesson learned

[3] Federal News Radio - https://federalnewsradio.com/health-it/2017/04/hhs-to-stand-up-its-own-version-of-the-nccic-for-health/

repository and the addition of over 1300 documents to enhance relevant situational awareness for end-users.

- A full methodology is under development for use in assessing the risks to the Sector including cyber, physical, and human vulnerabilities and threats.
- The PH SCC also maintains the standing workgroups on Risk Management and Cyber Security and Cyber Legislation.
- We participate in the reoccurring Health Care Industry Cybersecurity (HCIC) Task Force Meetings, which were established in 2016.
- Further, the SCC and GCC collaborated to establish a Joint Cyber Working Group to enhance cyber security engagement throughout the Sector.[4]

b. Do you get the sense that their role and contributions are understood and appreciated across the sector?

Answer: While many organizations are proactively engaged in the SCC more can, should, and must be done to bring in smaller partners with less resources. Effectively engaging with underfunded regional and local Health Sector partners so that they can contribute intelligence and benefit from information sharing to better protect the Health care sector from cyber vulnerabilities, remains an important goal.

c. Are there ways that the SCC could be more effective in assisting the sector with cybersecurity challenges?

Answer: Any mechanism to allow more collaboration across the Sector and between its key constituents within the ecosystem (government, public-private partnerships, health delivery organizations, manufacturers, associations, research entities, etc.) is truly welcome. This collaboration will lead to better alignment, which in turn will lead to better efficiency.

Question 3: My staff and I have heard from stakeholders in other industries, most notably the electricity sector, that they have broad, senior executive level engagement on their SCC, and that this engagement has significantly increased the effectiveness of the council and other aspects of their public-private partnerships, such as their ISAC. Who from your organization participates in the Health care SCC?

Answer: AdvaMed is represented in the SCC by President and CEO Scott Whitaker. Philips participates in the Health care SCC through myself, as Global Product Security Services Officer for Philips Healthcare.

a. Would a similar model, with broad senior executive engagement on the SCC, work in the health care sector? Why or why not?

[4] Health care and Public Health Sector-Specific Plan - May 2016: https://www.phe.gov/Preparedness/planning/cip/Documents/2016-hph-ssp.pdf

Answer: Each organization's C-Suite is different, so a one-size fits all approach would be difficult in manifesting appropriate participation across the industry by title alone. The intent of SCC membership and involvement should leverage the right leaders with the right skills and portfolios to adequately represent the sector, their organization and area of expertise in creating greater resiliency, and collaboration.

Participation in the SCC with appropriate executives would clearly be warranted to assure there is the broadest visibility at the highest levels within an organization. Philips, through current participation in different industry associations such as AdvaMed, is deeply engaged.

- Brent Shafer (CEO, North America) sits on AdvaMed's board
- Joe Robinson (Sr. VP Health Systems Solutions) is Chairman of the Board of MITA
- Michael McNeil (Global Product Security Services Officer) is on the board of directors for NH-ISAC as well as a participant In HHS Cybersecurity Task Force

Philips believes that establishing visibility with strong executives across these associations, is a worthwhile avenue for building a fruitful collaboration.

b. Do you have any other thoughts on the SCC and its importance or the roles it plays in health care sector cybersecurity?

Answer: As described in the SSP, the HPH Sector is large, diverse, and open, spanning both the public and private sectors. It includes publicly accessible health care facilities, research centers, suppliers, manufacturers, and other physical assets and vast, complex public-private information technology systems required for care delivery and to support the rapid, secure transmission and storage of large amounts of HPH data. Access to health care is critical in maintaining national health security. In 2011, Americans made 262 million visits to hospital emergency or outpatient departments. Over 14 million workers, representing more than 10 percent of the total American workforce, are employed in the HPH Sector throughout the U.S. This includes those who provide services directly to health care recipients and those who play a supporting role, such as vaccine manufacturers. Given this landscape, HPH Sector infrastructure security and resilience are ultimately defined by the ability of the Sector to prevent or mitigate negative impacts upon the delivery of HPH services. The SCC is integral in our ability to prepare, respond and recover from continued threats.[5]

Question 4: As the Sector Specific Agency for the health care sector, HHS has a big role to play in guiding and supporting industry cybersecurity efforts. Can each of you briefly tell us how HHS, as the SSA for your sector, provides cybersecurity guidance and support for your organization?

Answer: Under Presidential Policy Directive 21 (PPD-21), HHS has Sector-Specific Agency (SSA) responsibility for the Health care and Public Health (HPH) Sector. HHS implements its SSA role for the HPH Sector through the Critical Infrastructure Protection Program within the Office of the Assistant Secretary for Preparedness and Response (ASPR). Through these programs, HHS works in voluntary

[5] Health care and Public Health Sector-Specific Plan - https://www.phe.gov/Preparedness/planning/cip/Documents/2016-hph-ssp.pdf

partnership with public and private sector entities in the HPH and F&A Sectors to enhance their security and resilience with respect to all hazards, including cyber threats.

Beginning in 2014 HHS focused on increasing the Sector's awareness of the Cybersecurity Framework and implementing the Critical Infrastructure Cyber Community (C3) Voluntary Program within the Sector. HHS announced the release of the Framework through a website posting and presented on the Framework at major national Sector meetings. These meetings included the Public Health Preparedness Summit, Health care Information Management System Society (HIMSS) Conference, and Public Health Informatics Conference. The Sector has also tasked its standing Risk Management Working Group to develop the Sector's approach to the C3 Voluntary Program. The Sector's approach is focused on the cataloging and prioritization of federal resources for cybersecurity for Sector partners to access.[6]

Most recently and as the SSA for the Health care sector, HHS brought together members of the Health Care Industry Cybersecurity Task Force (initiated in 2016) of which I am a member. Our Task Force completed our report this month. Task Force members represent a wide variety of organizations within the health care and public health sector, including hospitals, insurers, patient advocates, security researchers, pharmacy and pharmaceutical companies, medical device manufacturers, health information technology developers and vendors, and laboratories. Many of my co-members are Chief Information Security Officers or equivalent positions within their organizations, while others have expertise in clinical medicine, software development, information security, and related fields.[7]

a. Who in HHS, or what office, is considered the "go-to" contact for cybersecurity issues?

Answer: Currently inside HHS, through the Health Care Industry Cybersecurity Task Force, Co-Chair is Emery Csulak, MS, CISSP, PMP, Chief Information Security Officer, Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services, is the 'go-to' contact. However, there clearly is not one official designated contact for cybersecurity issues that exists across all of HHS. And once the Cybersecurity Task Force is dissolved, Emory Csulak's responsibility will conclude. Therefore, this consideration must be addressed moving forward.

Question 5: My understanding is that there are multiple agencies within HHS that have pieces of health care cybersecurity. For example, the Office of Civil Rights deals with data breaches, the Food and Drug Administration deals with medical devices, and the list goes on for other components of the agency.

Answer: Correct - the response of the federal government to improving critical infrastructure cybersecurity in the health care sector is multi-pronged. Within the HHS, the Office for Civil Rights (OCR), CMS, the Food and Drug Administration (FDA), the Office of the National Coordinator (ONC), and the Office of the Assistant Secretary for Preparedness and Response (ASPR) play important and diverse roles in cybersecurity. Other administrative agencies and independent commissions, for example, the Federal Trade Commission (FTC) also play a role in setting expectations for privacy and security of health information.

---

[6] HHS activities to enhance cybersecurity - https://www.phe.gov/Preparedness/planning/cip/Pages/eo13636.aspx

[7] Health Care Industry Cybersecurity Task Force - https://www.phe.gov/Preparedness/planning/CyberTF/Pages/default.aspx

The multiplicity of actors in this space is often necessary to address a wide range of cybersecurity challenges and system types, and can be helpful in allowing these challenges to be viewed and addressed from multiple perspectives. It also has the potential to create complications. Some entities may be subject to regulation and oversight by multiple federal government entities, each with their own rules, which may be difficult to reconcile. Product and technology innovations for medical devices and health IT outpace the development and creation of regulations.[8]

a. Does this division of cybersecurity roles and responsibilities at HHS complicate the ability of Philips to address cybersecurity within its products and organization?

   Answer: Yes, while many regulations that apply to cybersecurity in health care are well-meaning and individually effective, taken together they can impose a substantial legal and technical burden on health care organizations. These organizations must continually review and interpret multiple regulations, some of which are vague, redundant, or both. In addition, organizations must dedicate resources to implement policy directives that may not have a material impact on reducing risks.[9]

b. Would additional coordination or clarity by HHS regarding which pieces of the agency have responsibility for cybersecurity, and when, help your organizations?

   Answer: Yes - Philips supports the Task Force recommendations on Improving Health Care Industry Cybersecurity (May 2017).

   Task Force Recommendation 1.1 - Create a cybersecurity leader role within HHS to align industry-facing efforts for health care cybersecurity.

   Currently many different programs and agencies within and outside of HHS are responsible for health care industry cybersecurity. While it is appropriate that different HHS components have their own roles and responsibilities based on their legislative authorities, it is also important to have a single person who is responsible for coordinating these activities. The benefits of this coordination include:

   - Allows one individual to look at cyber risks comprehensively, without being confined to specific program authorities, so that gaps can be more easily identified and addressed;
   - Provides a single point of entry for health care industry partners to discuss cybersecurity concerns with HHS, so that they may be directed toward the appropriate points of contact without having to navigate a complex organizational structure;
   - Helps prevent various components of HHS from engaging in conflicting or duplicative activities related to cybersecurity while promoting harmonization of regulations and guidance;
   - Promotes consistent cyber incident response with industry;

---

[8] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 11

[9] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 12

- Enables HHS to advocate more effectively for health care cybersecurity as a whole;
- Allows HHS to leverage cyber expertise from multiple programs; and
- Ensures that Vulnerability Equities Processes, or any process that replaces it, takes the specific rules and implications of health care technology into account.[10]

Task Force Recommendation 1.2 Establish a consistent, consensus-based health care-specific Cybersecurity Framework.

As we observed in other critical infrastructure sectors, a framework helped establish a consensus-based standard for improving the conversation around cybersecurity. Although NIST has developed a generic framework, health care (like other sectors) has many unique aspects such as its diverse resource capabilities, legacy systems that will persist for years, and the burden of low barriers for sharing of data that is essential for collaborative patient-oriented care. The framework should build upon the minimum standard of security required by the NIST Cybersecurity Framework and the HIPAA Security Rule to promote a single lexicon for the health care sector as well as standards, guidelines, and best practices. The complex environment requires certain basic standards that all stakeholders must meet and guidelines that allow flexibility for select issues. Without this framework, any of the countless constituents may pose a risk to the health care ecosystem.[11]

Task Force Recommendation 1.3 Require federal regulatory agencies to harmonize existing and future laws and regulations that affect health care industry cybersecurity.

The health care industry faces significant challenges due to federal and state cybersecurity laws and regulations that can be inconsistent and establish conflicting standards of compliance. These laws work in conjunction with laws on data breach notification, data disposal, and data security, often dictating different responses than federal laws. Additionally, complying with these laws and regulations is resource intensive and creates financial burdens for the health care ecosystem.

Because compliance with the various laws and regulations is burdensome, health care organizations often prioritize compliance over risk-based planning. A priority for regulatory agencies should be to ensure consistency among various federal and state cybersecurity regulations so that health care providers can focus on deploying their resources appropriately between securing patient information and the quality, safety, and accessibility of patient care instead of focusing on statutory and regulatory inconsistencies.

To demonstrate the complicated patchwork of laws, consider that in 2016, in addition to federal laws and regulations, members of the health care industry needed to adhere to computer crime laws touching upon issues such as:

- Unauthorized access, malware, and viruses in all 50 states;

---

[10] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 23

[11] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 24

- Denial of service attack laws in 25 states;
- Ransomware laws in two states, with another four states currently under consideration;
- Spyware laws in 20 states and two territories; and
- Phishing laws in 23 states and one territory [12]

c. Do you have any suggestions for actions that HHS could take to better coordinate or clarify its cybersecurity roles and responsibilities?

Answer: Yes - Philips supports the Task Force recommended Action Items on Improving Health Care Industry Cybersecurity.

Task Force Recommendation 1.1 Create a cybersecurity leader role within HHS to align industry-facing efforts for health care cybersecurity.

- Action Item 1.1.1: The HHS Secretary must name and resource a cybersecurity leader for sector engagement.
- Action Item 1.1.2: The HHS Secretary must task the cybersecurity leader to work with federal, state, and industry partners to create a plan to establish goals and priorities for health care sector cybersecurity.
- Action Item 1.1.3: The HHS Secretary must authorize the cybersecurity leader to define the reporting lines directly to other federal agencies tasked with cybersecurity such as the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and others.
- Action Item 1.1.4: The cybersecurity leader must assist in streamlining HHS' outreach in a consistent manner to industry (e.g., branding, alignment with the NIST Cybersecurity Framework).
- Action Item 1.1.5: The cybersecurity leader should establish a mechanism for partnering with and gathering industry input to prioritize short- and long-term goals, such as a federal advisory committee or similar mechanism.
- Action Item 1.1.6: The cybersecurity leader should coordinate with U.S. and international intelligence agencies to ensure that Vulnerability Equities Process-like processes respect the special nature of digital health technology. Additionally, the cybersecurity leader should contribute to ongoing international policymaking and best practice development in this area.[13]

Task Force Recommendation 1.2 Establish a consistent, consensus-based health care-specific Cybersecurity Framework.

- Action Item 1.2.1: HHS should complete work on the Act Section 405 (d) for Aligning Health Care Industry Security Approaches through a consensus-based approach to develop a health care sector specific cybersecurity framework.
- Action Item 1.2.2: HHS and NIST must develop guidance about how to apply the framework to the health care sector.

---

[12] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 25

[13] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 24

- Action Item 1.2.3: Industry and government should partner to establish an evaluation mechanism and prioritized best practices to support the range of small to large organizations to consistently apply the NIST Cybersecurity Framework.[14]

Task Force Recommendation 1.3 Require federal regulatory agencies to harmonize existing and future laws and regulations that affect health care industry cybersecurity.

- Action Item 1.3.1: HHS, in coordination with the private sector, federal, and state partners should look across HHS to harmonize regulations that directly or indirectly apply cybersecurity standards or best practices to reduce the burden on the industry.
- Action Item 1.3.2: HHS should make recommendations to Congress about required statutory changes.
- Action Item 1.3.3: HHS must publish standards and guidance consistent with the NIST Cybersecurity Framework. These should be developed based on the structure of the framework, as opposed to a mapping after the fact.36
- Action Item 1.3.4: HHS should establish a Task Force to explore options to incentivize risk-based cybersecurity in alignment with their existing oversight roles.
- Action Item 1.3.5: HHS should develop a conformity assessment model37 built upon a public/private partnership to standardize cybersecurity compliance consistently across programs. Conformity assessments conducted by private sector organizations can increase productivity and efficiency and by encouraging federal agencies to standardize expectations.[15]

Question 6: The public-private partnership model depends on trust and collaboration between government and private sector participants. This can prove challenging in some sectors, such as health care, where the Sector Specific Agency (SSA) is also the regulator for that sector. Some sectors — such as financial services — have overcome these challenges to develop a robust relationship with their SSA. How much does the success of a public private partnership for cybersecurity depend on the level of trust and collaboration between private sector participants and their government counterparts, especially their sector specific agency?

Answer: We found that the public-private partnership cultivated by the Task Force, which resulted in the development of the Report on Improving Health Care Industry Cybersecurity, has provided an opportunity to address significant cybersecurity concerns in the health care industry. The Task Force members found this engagement with other federal and private sector partners beneficial to understand our common cybersecurity challenges and concerns. Therefore, we believe the establishment of an ongoing public-private forum would serve to enhance cybersecurity discussions and protections as a critical component for the health care industry to increase patient safety.[16]

a. Is this a challenge in the health care sector, where HHS is the Sector Specific Agency but also serves as the regulator?

---

[14] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 24
[15] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 25
[16] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 4

Answer: We wholeheartedly support full participation within the public-private sector and agree trust is paramount for any type of major information sharing in that environment. We do find that there are sometimes obstacles to realizing that trust when your government regulatory agency is a participant. However, the role of HHS is critical and we are 100% supportive of their participation in this process. If we have the ability to leverage lessons learned from other industries or sectors who have overcome similar challenges, we must take full advantage.

One of the best working relationships Philips has is with the FDA as they conduct their workshops. We have the FDA currently participating in their 'memorandum of understanding', with the NH-ISAC and the Medical Device Innovation Safety and Security organization (MDISS). This brings manufacturers, researchers, technologists and regulators to the same table in order to develop an information sharing model – the MD-VIPER.

As mentioned before, it is important that HHS identify a single point of contact to coordinate with the private sector, federal, and state partners to harmonize regulations that directly or indirectly apply cybersecurity standards or best practices.

b. Does the fact that different parts of the health care sector are regulated by different components of HHS complicate this relationship?

Answer: Yes. As discussed in our Report the multiplicity of actors in this space is often necessary to address a wide range of cybersecurity challenges and system types, and can be helpful in allowing these challenges to be viewed and addressed from multiple perspectives. It also has the potential to create complications. Some entities may be subject to regulation and oversight by multiple federal government entities, each with their own rules, which may be difficult to reconcile. Product and technology innovations for medical devices and health IT outpace the development and creation of regulations. While many regulations that apply to cybersecurity in health care are well- meaning and individually effective, taken together they can impose a substantial legal and technical burden on health care organizations. These organizations must continually review and interpret multiple regulations, some of which are vague, redundant, or both. In addition, organizations must dedicate resources to implement policy directives that may not have a material impact on reducing risks.

At the same time, gaps in protections can leave key health care issues unaddressed and create holes in cybersecurity infrastructure for health information. Consider, for example, the different roles of FDA and OCR with respect to health information cybersecurity. FDA is charged with ensuring approved and cleared medical devices are safe and efficacious, whereas OCR is charged with oversight of the privacy and security regulations under HIPAA, which applies only to "covered entities" (e.g., most health care providers, health plans, and health care clearinghouses), and contractors acting on their behalf, known as "business associates." With the recent publication of the FDA's final guidance for manufacturers on device cybersecurity, the FDA has taken more steps to address the patient safety concerns generated by cybersecurity risks to medical devices. However, FDA oversight is limited to patient safety and does not extend to patient privacy. HIPAA's regulations focus on both privacy and security; however, medical device manufacturers may not be covered entities or business associates under HIPAA. This leaves a health care provider using a medical device with potentially greater responsibility for assuring privacy and security protections

for health information created and shared by the device. While many stakeholders agree that protecting against cybersecurity threats should be a shared responsibility, to date, health care providers have shouldered an inordinate amount of the burden even when actions needed to improve security in the device have been outside their control.

The challenges around the push and pull of the regulatory complexity associated with ensuring patient safety and patient privacy is growing with an increasing amount of information that is being shared digitally and the proliferation of the use of devices. The Health Information Technology for Economic and Clinical Health Act spurred investment in EHRs through billions of dollars of incentives to hospitals and clinicians under the "Meaningful Use" of EHR program. The Meaningful Use program combined with the Merit-Based Incentive Payment System will continue to push providers to use EHRs and other technologies to exchange patient information electronically. In addition, alternate payment models of care which rely heavily on the use of health IT combined with the increased capacity of medical devices to store a growing amount of PHI, means more patient data is at risk for cybersecurity attacks. Data collected for the good of the patients and used to develop new treatments can also increase cybersecurity risks to the health care system.

However, to date there has been little focus on cybersecurity – while at the same time, the techniques being used by cyber criminals are growing increasingly sophisticated. According to a recent KLAS12 report, many survey respondents widely reported that their EHRs placed little attention on cybersecurity. Providers also report that many device manufacturers treat security as either an afterthought or that the attention is woefully inadequate.[17]

c. Based on your experience, have other industries managed to navigate a similar situation, where their Sector Specific Agency is also their regulator? Or are there challenges unique to the health care sector its relationship to HHS that further complicate this dynamic?

Answer: Our sector is not unique in being regulated by our SSA. For example, the US Department of Treasury functions as the SSA for the finance sector and U.S. Department of Energy (DOE) for the Energy sector. The Health care community routinely shares best practices across sectors to leverage lessons learned and strengthen our capabilities. For example, last month members of the community heard from our counterparts from these two industries at the Health Care Industry Cybersecurity (HCIC) Task Force Meeting held at HHS on April 21st.

Our speakers from the Finance and Energy sectors included:

- Brian Peretti, Director, Office of Critical Infrastructure Protection and Compliance Policy, U.S. Department of the Treasury
- John Carlson, Chief of Staff, Financial Services Information Sharing and Analysis Center
- Mike Smith, Senior Cyber Policy Advisor, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy (DOE)

[17] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 12

- Fowad Muneer, Program Manager, Office of Electricity Delivery and Energy Reliability, DOE
  Nadya Bartol, Vice President, Industry Affairs and Security Strategist, Utilities Telecom Council[18]

At a macro level one assumes challenges in coordination between regulator and industry. We have found similarities as well as differences in meeting with our counterparts from different sectors.

Currently in the HC sector, medical devices are deployed in a clinical setting. We do not yet have, but should have a medical certification that rates the vulnerabilities specific to those products. HHS should develop a conformity assessment model built upon a public/private partnership to standardize cybersecurity compliance.

The FDA is the overarching governing body for medical device manufacturers as well as pharmaceutical companies, but the CMS is the governing body over the health delivery organizations. This dichotomy can lead to unintentional regulatory/guidance confusion.

Question 7: Your organization is obviously larger and more well-resourced than a rural hospital or small physician practice. We've seen in other cases like the Target breach, however, that smaller organizations can be the "infection points" for larger organizations, due to the way that business relationships and networks are set up. Recognizing that cybersecurity is a collective responsibility, how do — or can — larger organizations assist in bolstering awareness and engagement of smaller participants in the sector?

Answer: The Federal government along with health care industry leaders can have a profound impact on the resilience of the entire industry through collaboration. We have specifically outlined several action items in our Report including those found in Imperative 4, which is described below.

Imperative 4: "Increase health care industry readiness through improved cybersecurity awareness and education."

Cybersecurity can be an enabler for the health care industry, supporting both its business and clinical objectives, as well as facilitating the delivery of efficient, high-quality patient care. However, this requires a holistic cybersecurity strategy. Organizations that do not adopt a holistic strategy not only put their data, organizations, and reputation at risk, but also—most importantly—the welfare and safety of their patients.

Cybersecurity must be governed with a collaborative approach whereby all members of the health care industry work together toward the common goal of protecting one another and the sector's most critical assets – patients. To achieve this requires an educated workforce and an informed public who make evidence-based decisions that are reliant on cyber-secure data. As part of this holistic security strategy, it is critical that a thorough baseline is established whereby inherent trust can be established between patients and providers, technologies and processes, and ultimately institutions and patients.

---

[18] **Summary:** Health Care Industry Cybersecurity Task Force Meeting Summary - April 21, 2016

This will lead to a high level of confidence in which the industry understands cybersecurity hygiene and ultimately establishes trust throughout the health care continuum. Once a baseline level of hygiene is established, the industry must come together to develop a methodology to audit, measure, and continually steer the industry progressively forward

The health care industry must increase outreach for cybersecurity across all members of the health care workforce through ongoing workshops, meetings, conferences, and tabletop exercises. Additionally, the health care industry must provide patients with information on how to manage their health care data by developing consumer grading systems for non-regulated health care services and products. Lastly, the health care industry must develop cyber literacy programs to educate decision makers, executives, and boards of directors about the importance of cybersecurity education. [19]

a. Are there factors that impede collaboration within the sector?

Answer: Yes. One example is the awareness that cybersecurity risks and threats are inconsistently understood across the sector when making both personal and organizational decisions regarding cybersecurity.[20] The susceptibility to cyber threats exists for many organizations because most people are neither aware of the risks, nor have the tools to protect their systems. Cybersecurity is a shared responsibility that requires diligence from all who interact with or facilitate the collection, maintenance, and exchange of health care information and use interconnected medical systems. Poor cybersecurity practices at any level can become the cause of a breach and leave patients exposed to unexpected harm to their privacy or even the care they receive.

There is currently a lack of shared awareness of cybersecurity risks and best practices among health care systems. The health care sector should engage with HHS and DHS to build on the established National Cybersecurity Awareness Campaign to ensure broad outreach to the sector and develop a baseline cybersecurity understanding at all levels, as well as tailored information for health care executives, clinical providers, patients, and other key groups that may not possess fluency in IT matters. This awareness will provide them the ability to use health care IT in a risk-informed manner so they can take the necessary steps to better protect health care information.[21]

Question 8: Are there lessons from the progress of cybersecurity in the medical device sector that can benefit other parts of the health care sector, as well as the sector as a whole? If so, what are some of these lessons?

Answer: Yes. One such example would be the development of the Medical Device Vulnerability Intelligence Program for Evaluation and Response (MD-VIPER). The goal of the program is to create an open community of Medical Device Cybersecurity stakeholders (Manufacturers, Health care Delivery

---

[19] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 40

[20] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 41

[21] Health Care Industry Cybersecurity Task Force Report on Improving Health Care Industry Cybersecurity - Page 44

Organizations, Independent Security Researchers, Regulatory Agencies, etc.) to promote a consensus & consistency of approach and process, to contribute significantly to Medical Device Cybersecurity education, as well as to foster situational awareness of Medical Device threats, best practices and mitigation strategies.

The MD-VIPER portal is hosted by the HS-ISAC, the reporting process is:

- Vulnerability reporting agent contacts MD-VIPER
- Conversation between reporting agent and MD-VIPER
- Reporting agent proceeds with sharing of vulnerability
- Once vulnerability is reported, all data is stationary until a data owner, manufacturer, advises in writing to share the data
- If a third party shares the data, they should be able to advise us, in writing, to share the data

Participation in MD-VIPER is:

- Open to all medical device security stakeholders
- Free and voluntary (once registration and NDA process are complete)
- Tracking each event (submissions, data sharing event, communication event, etc.)
- Each event is triggered by the manufacturer
- Collaboration with manufacturer
- Responsible sharing of information regarding vulnerabilities and threats in light of specified vulnerabilities for stakeholder awareness

Question 9: During the hearing, we talked a great deal about the HHS as the SSA, and the NH-ISAC, but we didn't really touch on the Government Coordinating Council. What role does the GCC play for each of your organizations?

Answer: The work of the Health care and Public Health GCC includes, but is not limited to: 1) contributing information and data, and recruiting subject matter experts as needed to assist in the development and execution of the Sector Specific Plan (an annex to the NIPP) and Sector Annual Report; 2) collaborating with its private sector counterpart, the sec, to identify, prioritize and protect sector critical infrastructure; 3) collaborating with those sectors responsible for protection of assets, systems, networks, or services upon which the health care and public health sector is dependent; and 4) assisting in the development of products as requested by the Department of Homeland Security (DHS).

The GCC will work toward accomplishing the following goals:

1. The GCC membership will "leverage relationships and resources to assess and analyze threats to vulnerabilities of, and consequences to HPH Sector critical infrastructure to inform risk management activities. Ensure that approaches consider the physical, cyber, and human elements of critical infrastructure security and resilience, supply chain issues and interdependencies with other sectors".
2. The GCC membership will "execute risk mitigation activities in a prioritized manner with clear plans and metrics for success".
3. The GCC membership will "enhance existing and develop new mechanisms to ensure bidirectional sharing of information".
4. The GCC membership will "exercise the ability of the sector to respond to natural or manmade disasters and incorporate lessons learned into future exercises and corrective actions". ·

5. The GCC membership will "regularly review and assess the active roster of participating members to ensure appropriate representation is maintained to enhance sector resilience, facilitate necessary information sharing within the public sector and private sector offices and respond to emergency events".[22]

   a. Are there additional initiatives that you believe that the GCC could take, or roles that it could fill, that would help your organizations and the health care sector as a whole better address cybersecurity?

      Answer: Neither Philips nor AdvaMed are current members of the Government Coordinating Council, however the Council's success will build upon the notion that public-private partnerships can help realign certain agencies inside the government to more efficiently address the challenges of cybersecurity.

Question 10: Would you support HHS making a recommendation that encourages participation in ISAC?

Answer: Yes, I would. Philips would also support the Department's enthusiastic recommendation to OEMs to join the HS-ISAC without reservation.

We concur with the submitted testimony on behalf of the MH-ISAC: "One of the greatest challenges for the NH-ISAC and all ISACs is the lack of awareness amongst the critical infrastructure owners and operators, particularly the smaller owners and operators, that the ISACs exist and are a valuable tool. Numerous incidents have shown that effective information sharing amongst robust trusted networks of members works in combatting cyber threats.

Government, and specifically the Sector Specific Agencies (SSAs) should regularly and consistently encourage owner/operators and especially at the Board and CEO level to join their respective ISACs. This has been very effective in the financial sector where the United States Department of the Treasury, the regulators and state agencies have been strongly encouraging membership in the FS-ISAC as a best practice. Currently, not all SSAs support their sector designated ISACs in the same manner."[23]

   a. Do you believe that it would improve the functioning of the ISAC, and therefore cybersecurity across the sector, for HHS to make such a recommendation?

      Answer: Yes. A recommendation from HHS for Health care OEMs to join the HS-IASC would directly benefit our combined efforts. As I stated in my prepared testimony "we commend the FDA for its proactive leadership role over medical device cybersecurity. The FDA has worked closely with the medical technology industry and the broader health care ecosystem to ensure medical device cybersecurity is considered and addressed throughout all stages of product design and use the FDA entered into a Memorandum of Understanding ("MOU") with the National Health

---

[22] Health care and Public Health Sector Government Coordinating Council Charter - Pages 2-3
[23] Testimony of Denise Anderson On Behalf of the National Health Information Sharing & Analysis Center - http://docs.house.gov/meetings/IF/IF02/20170404/105831/HHRG-115-IF02-Wstate-AndersonD-20170404.pdf

Information Sharing and Analysis Organization ("NH-ISAC") and the Medical Device Innovation, Safety and Security Consortium ("MDISS") to promote cybersecurity information sharing for medical devices."[24] As I relayed in my written testimony HS-IASC has recently launched a program called the Medical Device Vulnerability Intelligence Program for Evaluation and Response, or MD-VIPER. MD-VIPER provides a streamlined mechanism for medical device manufacturers to submit and share information concerning cybersecurity-related issues, as well as other members of the broader health care ecosystem.

b. Do you think there are potential consequences — real or perceived — from HHS taking this approach?

Answer: In light of the FDA's significant work and achievements to date, and the Agency's staff ongoing engagement with industry, we believe that the FDA's collaboration with the MS-IASC serves as an example to all regulatory bodies with respect to the type of interaction, collaboration, and guidance an agency should provide to its regulated industry.

Question 11: Recently in the cybersecurity community, there has been some confusion regarding ISACs and ISAOs. Do you think that this confusion has caused any issues with regards to cybersecurity protocol — specifically facilitating effective situational awareness and response activities, particularly when an incident occurs?

Answer: During her testimony, National Health Information Sharing and Analysis Center (NH-ISAC) President Denise Anderson stated that the confusion between the ISAC definition and the ISAO definition must be eliminated.[25]

As you are aware the Department of Homeland Security states an ISAO is a group created to gather, analyze, and disseminate cyber threat information. Unlike ISACs, ISAOs are not directly tied to critical infrastructure sectors, as outlined in Presidential Policy Directive 21. ISAOs offer a more flexible approach to self-organized information sharing activities amongst communities of interest such as small businesses across sectors: legal, accounting, and consulting firms that support cross-sector clients, etc. [26]
ISAOs are useful communities. However, the flexibility within the construct of an ISAO that allows for broader communications, lacks protections that encourage vigorous sharing of information.

During the hearing, Denise Anderson stated: "ISACs offer several vehicles to share effective techniques and practices for preventing, detecting and managing cyber security risk that are often un-conventional controls (definition: controls that are designed and implemented independent of any risk framework, standard or regulatory guidance), ISAOs don't offer vehicles for this type of sharing."

a. What do you think should be done to address this confusion?

---

[24] Michael C. McNeil, Philips - AdvaMed, the Advanced Medical Technology Association Testimony - http://docs.house.gov/meetings/IF/IF02/20170404/105831/HHRG-115-IF02-Wstate-McNeilM-20170404.pdf

[25] Health IT Security - http://healthitsecurity.com/news/health care-information-sharing-need-stressed-in-recent-hearing

[26] DHS FAQ on ISAOs - https://www.dhs.gov/isao-faq

Answer: As Denise Anderson stated at the hearing the government can **aid information sharing** by encouraging owners and operators of critical infrastructure to join their respective sector ISACs and to offer financial incentives (i.e. tax breaks) for owners and operators to join ISACs.

Furthermore, the government can:

- Recognize ISACs and the role that they play in critical infrastructure protection and resilience
- Protect information sharing by ensuring data shared amongst members is protected
- Place strong, defined and permanent cybersecurity liaisons and leadership within the SSAs to advocate the public private partnership when it comes to cyber matters

Information sharing is designed to "create situational awareness" so risk-based decisions can be made. It should also "allow operational components within owner/operation organizations that have direct actionable control over the content they are sharing, to perform an action. The focus needs to be on enhancing the ability of operational groups to work closely with each other."[27]

###

[27] Health IT Security - http://healthitsecurity.com/news/health care-information-sharing-need-stressed-in-recent-hearing