U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

April 1, 2017

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing on "Cybersecurity in the Heath Care Sector: Strengthening Public-Private Partnerships"

I. INTRODUCTION

On Tuesday, April 4, 2017, at 10:15 a.m. in 2322 Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing entitled "Cybersecurity in the Heath Care Sector: Strengthening Public-Private Partnerships." This hearing will examine the current state of public-private partnerships for cybersecurity in health care, one of 16 critical infrastructure sectors. Health care has long struggled to coalesce around the institutions and infrastructure necessary to improve the security posture of the industry due to several complex factors. This hearing presents an opportunity to explore the challenges in health care cybersecurity and to identify opportunities to improve leadership and engagement across the sector.

II. WITNESSES

- Denise Anderson, President, National Health Information Sharing and Analysis Center;
- Michael McNeil, Global Product Security & Services Officer, Royal Philips; and,
- Terry Rice, Vice President, IT Risk Management & Chief Information Security Officer, Merck & Co., Inc.

III. BACKGROUND

A. Cybersecurity and the Public-Private Partnership Model

Cybersecurity is a broad, dynamic, and rapidly evolving challenge for modern society. As we become more dependent on the Internet and information technologies, cyber threats will continue to proliferate at an exponential rate and the consequences of incidents will become increasingly profound. The evolution of cyber-physical systems such as cars, medical devices, the electric grid, and other connected consumer products not only increase the attack surface, but also escalate the threat from loss of information to potential physical harm.

Given the scope and scale of society's dependence on connected technologies and the attendant cyber threat, cybersecurity is not something that can be "solved." As the threats proliferate and consequences become more severe, however, it is paramount that the nation

strengthen its approach to cybersecurity. The challenge lies in the fact that there is no single solution to better cybersecurity; it depends on multiple improvements, new approaches, and fresh thinking, as well as a commitment to strengthening existing institutions. A key factor is the coordination and engagement between government and private sector partners. After all, while it is the public sector's responsibility to protect critical infrastructure for the safety and security of society, 85% of that infrastructure is owned and operated by the private sector.[1] Thus, the relationships between the public and private sectors depend on a combination of trust, leadership, and commitment from both sides.

To facilitate this relationship, the United States relies on a public-private partnership model that has evolved over the last two decades.[2] In this model, the private sector is split into 16 critical infrastructure sectors, each of which in turn relies on four organizations either identified or created within the model; a Sector Specific Agency (SSA), a Government Coordinating Council (GCC), a Sector Coordinating Council (SCC), and an Information Sharing and Analysis Center (ISAC). Each of these organizations plays a unique and complimentary role in helping to shape and guide cybersecurity efforts throughout the sector.

- **Sector Specific Agencies (SSAs):** For each sector, SSAs are tasked with representing and advocating for their sector's unique equities, providing support and guidance to their industry stakeholders, and implementing government-wide cybersecurity initiatives and strategies.[3]

- **Government Coordinating Councils (GCCs):** Led by a sector's SSA, GCCs bring together government stakeholders from federal, state, local, territorial, and tribal agencies to help coordinate and deconflict government efforts.

- **Sector Coordinating Councils (SCCs):** Comprised of industry stakeholders from across the sector, SCCs are tasked with representing industry equities and needs, guiding and coordinating efforts among industry to address issues, and working with their designated SSA and GCC to help implement initiatives and mandates.

- **Information Sharing and Analysis Centers (ISACs):** ISACs are meant to improve the cybersecurity of industries through the establishment of organizations whose primary purpose is to collect, analyze, and disseminate cybersecurity threat information. This information may then be shared between stakeholders.

B. The Current Landscape of the Public-Private Partnership Model

Every sector has unique characteristics and challenges that influence the success of the public-private partnership model. While the motivations for and paths to success differ across

1 *Critical Infrastructure and Key Resources*, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, PARTNER ENGAGEMENT, https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources.
2 Over the course of the last two decades, the executive branch has issued a series of documents that either established or refined this model, including: Homeland Security Presidential Directive (HSD-7), Presidential Policy Directive 21 (PPD-21), and PPD-41. These in turn led to the design and implementation of the National Infrastructure Protection Plan (NIPP) and the National Cyber Incident Response Plan (NCIRP).
3 *Id*.

sectors, those that are regarded as the most effective share similar traits. Specifically, they have robust engagement with their SSA and widespread buy-in from private industry across the sector. For example, in recent years the energy sector improved engagement and performance of its public-private institutions, including the E-ISAC, due to broad senior executive level representation on the SCC.[4] This has improved engagement across the sector and facilitated more effective collaboration with government partners at their SSA, the Department of Energy.[5] The Financial Services sector has experienced similar successes with the Financial Services-ISAC (FS-ISAC) and Financial Services-SCC (FSSCC) by fostering a strong relationship with its SSA, the Department of the Treasury, and by ensuring that industry engages regularly and effectively with both the FS-ISAC and FSSCC.[6]

By creating institutions where both public and private stakeholders actively coordinate efforts—as well as share information, incidents, and feedback—cybersecurity challenges that arise within the sector may be quickly addressed in a collaborative fashion. This helps reduce misunderstandings between the public and private sectors when cybersecurity incidents occur, facilitates the timely sharing of important information between stakeholders, and ensures that both public and private sector equities are considered. Critical infrastructure sectors like financial services, which includes small community-oriented credit unions all the way up to large multi-national enterprises like Chase Bank, and health care, which includes rural hospitals, physician offices, and large insurance companies, are incredibly diverse. Further, for both sectors, their SSA is also their industry regulator. In comparison to a more homogenous sector like energy, this creates additional challenges for these sectors when leveraging the public-private partnership model. However, these examples are instructive of the benefits that result from strong leadership and prioritization of cybersecurity across a sector.

C. Health Care Cybersecurity and the Public-Private Partnership Model

The health care sector has been considered critical infrastructure for nearly twenty years, and has been successful in leveraging public-private partnerships in areas like physical security and disaster preparedness.[7] It has struggled to fully establish and leverage these institutions and partnerships with regards to cybersecurity, however. This is partially attributable to the fact that cybersecurity is a relatively new challenge for much of the health sector. In recent years, as the sector has become more digitized and therefore increasingly vulnerable to cybersecurity threats, the need for strong cybersecurity has become apparent. Large-scale malware infections, data breaches, and publicly-revealed vulnerabilities in medical devices are more frequent, adding

---

4 Written Testimony, Scott Aaronson, Exec. Dir., Security and Business Continuity, Edison Electric Institute, before the House Comm. on Energy and Commerce, S.Comm on Energy (February 1, 2017), at 7.
5 *Id.*
6 Written Testimony, Gregory T. Garcia, Advisor, Financial Services Information Sharing and Analysis Center, before the House Comm. on Financial Services, S.Comm on Financial Institutions and Consumer Credit (March 5, 2014), at 3.
7 Healthcare and Public Health Sector-Specific Plan (May 2016), *available at* https://www.phe.gov/Preparedness/planning/cip/Documents/2016-hph-ssp.pdf.

scrutiny and pressure to improve cybersecurity.[8,9] This will only increase as technology continues to transform the sector.

While much of the sector now recognizes its vulnerability to this threat, efforts to increase cybersecurity are sporadic, overly narrow, or become conflated with issues such as privacy or compliance, reducing their effectiveness.[10] This has several causes, including the fact that different parts of the health care sector are regulated by different agencies within the Department of Health and Human Services (HHS), existing regulation and legislation around medical privacy and cybersecurity such as the Health Information Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), and the variety of actors within the sector, to include healthcare delivery organizations, insurance companies, and patients themselves.[11]

The diversity and complexity of the industry has affected the ability of cybersecurifocused public-private partnerships to take root. Organizations like the National Health Information Sharing and Analysis Center (NH-ISAC) and Health Care and Public Health Sector Coordinating Council (HPH-SCC) have strived to improve their cybersecurity capabilities in an effort to become as effective as their counterparts in other sectors. The NH-ISAC has existed since 2010, for example, but has apparently been forced to reconstitute to improve performance. While meaningful progress has recently been made, partially because of the appointment of an ISAC veteran as president, work remains to equip the ISAC with the organizational, fiscal, and technical capabilities it needs.[12] Similar works remains with the HPH-SCC. Finally, the distributed nature of cybersecurity regulatory and oversight responsibilities at HHS—the SSA for health care—has contributed to a lack of coordinated, comprehensive leadership, which in turn has had ripple effects across the sector as stakeholders struggle to understand their roles and responsibilities.

i. A Successful "Case Study": The Medical Device Industry

While the broader health care sector has struggled to fully establish and leverage the public-private partnership model, the medical device industry has achieved success in its recent efforts to replicate the model within its subsector. The industry's regulator, the Food and Drug Administration (FDA), has essentially taken on the role of a medical device subsector "SSA" and has taken a forward-leaning, collaborative approach to medical device cybersecurity. FDA engages in regular discussions with its stakeholders, solicits and incorporates feedback into its processes and guidance, and maintains a visible, active presence with regards to cybersecurity

---

8 Marla Durben Hirsch, *Cybersecurity: What 2016 taught the healthcare industry*, FIERCEHEALTHCARE, Dec. 19, 2016, http://www.fiercehealthcare.com/it/feature-cybersecurity-what-2016-teaching-industry.
9 Neil Versel, *'Cybersecurity has become a full-time job' in healthcare*, MEDCITYNEWS, Nov. 28, 2016, http://medcitynews.com/2016/11/cybersecurity-full-time-job-healthcare/.
10 *See supra* note 8, 9.
11 *Id.*
12 Marianne Kolbasuk MeGee, *HHS to Fund a Cyber Threat Information Sharing Leader*, BANKINFOSECURITY, Aug. 1, 2016, http://www.bankinfosecurity.com/hhs-to-fund-cyber-threat-information-sharing-leader-a-9300.

issues and incidents.[13,14] Industry stakeholders, in addition to their robust engagement with FDA, regularly communicate at the senior executive level in ways very similar to an SCC. Finally, the industry has recently constituted an Information Sharing and Analysis Organization (ISAO), functionally like an ISAC, that focuses on medical device cybersecurity threats.[15]

In replicating the public-private partnership model within the subsector, the medical device industry has been able to quickly increase the cybersecurity posture of the subsector as a whole.[16] While much work remains to be in done, by embracing this model, the industry and FDA have created a strong foundation on which to continue to improve the subsector's cybersecurity. The recent progress within the medical device sector may provide instructive lessons for the broader health care sector as it looks to strengthen engagement in public-private partnerships.

This hearing will explore ways to strengthen the NH-ISAC and HPH-SCC, to include steps that the public and private sectors may take to better support and leverage these organizations. In addition, this hearing will examine HHS's role as the SSA and whether there are additional actions that the agency may take to contribute to improved cybersecurity across the health care sector.

IV. ISSUES

- Are there additional ways that HHS can be a more effective SSA for the health care sector?
- How can the NH-ISAC be strengthened and better supported?
- How can the HPH-SCC better represent and respond to the needs of industry?
- Are there "lessons learned" that the health care sector may adapt from the medical device subsector or energy and financial services sectors?

V. STAFF CONTACTS

Please contact Jessica Wilkerson or John Ohly of the Committee staff at (202) 225-2927 with any questions.

---

13 Suzanne B. Schwartz, M.D., M.B.A., *Managing Medical Device Cybersecurity in the Postmarket: At the Crossroads of Cyber-safety and Advancing Technology*, FDA VOICE, Dec. 27, 2016, https://blogs.fda.gov/fdavoice/index.php/2016/12/managing-medical-device-cybersecurity-in-the-postmarket-at-the-crossroads-of-cyber-safety-and-advancing-technology/.
14 Christian Dameff et al., *State of Healthcare Cyber Security*, BSIDESLV 2016, Aug. 2, 2016, https://www.youtube.com/watch?v=JjHSUKWRtlo&app=desktop.
15 Christina Hwang, *FDA's MD-VIPER to help device stakeholders with cybersecurity vulnerabilities*, HEALTHCAREBUSINESS DAILY NEWS, Feb. 2, 2017, https://www.dotmed.com/news/story/35207.
16 *See supra* notes 12, 13, 14.