MEMO

To: AEHIS Members and the AEHIS Public Policy Committee Members
From: CHIME Public Policy
Re: Recap of April 4, 2017, Energy & Commerce Committee Hearing, "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships"

Takeaways:

- Bipartisan interest in healthcare cybersecurity exists
- Committee members acknowledged the variations in capabilities and resources across the industry, especially small and rural providers
- Medical Device cybersecurity is on Congress' radar, but they think there is more than adequate FDA-industry coordination
- NH-ISAC wants to grow, is offering free trial memberships and discounted rates as low as $1,200/year

Witnesses:

- Denise Anderson, President, National Health Information Sharing and Analysis Center
- Michael McNeil, Global Product Security & Services Officer, Philips (On behalf of the Advanced Medical Technology Association, AdvaMed)
- Terry Rice, Vice President, IT Risk Management & Chief Information Security Officer, Merck & Company, Inc.

Committee Members in Attendance:
Subcommittee Chairman Tim Murphy (R-PA), Subcommittee Ranking Member Diana DeGette (D-CO), Full Committee Chairman Greg Walden (R-OR), Full Committee Ranking Member Frank Pallone (D-NJ), Jan Schakowsky (D-IL), Morgan Griffith (R-VA), Michael Burgess (R-TX), Yvette Clarke (D-NY), Susan Brooks (R-IN), Chris Collins (R-NY), Raul Ruiz (D-CA), Mimi Walters (R-CA), Ryan Costello (R-PA), Buddy Carter (R-GA)

Summary:
On April 4, 2017, the House Committee on Energy & Commerce, Subcommittee on Oversight & Investigations held a hearing entitled, "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships." The hearing marked the first healthcare-focused cybersecurity conversation during the 115th Congress.

The hearing was broadly focused on public-private collaboration on healthcare cybersecurity, with a focus on the National Health Information Sharing and Analysis Center (NH-ISAC) and the Sector Coordinating Council (SCC) led out of the Department of Health and Human Services (HHS.)

Chairman Murphy opened the hearing by highlighting the challenge of healthcare cybersecurity, he urged that given the rapid digitization of the industry, cybersecurity must be a priority. On the NH-ISAC, he questioned what the value proposition is for small and rural hospitals.

Ranking Member DeGette offered opening remarks citing the volume of medical records breached and the importance of leveraging experience in other industries to evaluate the role of the NH-ISAC. She also reminded the Committee about the letter she and Congresswoman Brooks sent to the FDA concerning medical device cybersecurity that has not yet been responded to.

Chairman Walden called public-private collaboration “vital” for healthcare cybersecurity. He suggested the industry focus on risk minimization.

Ranking Member Pallone cited the severity and frequency of the attacks on the industry.

Denise Anderson was the first witness to offer testimony. She cited the Memorandum of Understanding (MOU) with the FDA, NH-ISAC and (Medical Device Innovation, Safety and Security Consortium) MDISS as an example of successful public-private collaboration. She said that privacy was the old focus of the industry and called for that to evolve. She suggested 4 activities to improve the stature of the industry: 1. Education about the NH-ISAC and information sharing broadly and among senior leadership within healthcare organizations and to encourage participation in ISACs through incentives; 2. Protections for information sharing, from subpoena and legal enforcement; 3. Clarification about the differences between ISACs and Information Sharing and Analysis Organizations (ISAOs.); 4. Senior cybersecurity liaisons within Sector Specific Agencies, in healthcare it would be HHS.

Michael McNeil said that the industry can’t just stay on top of threats but cited the importance of collaboration with regulators and healthcare providers. He said that the medical device manufacturers must: 1. Leverage medical device risk management – both in design and maintenance of medical devices; 2. System level security – following the AdvaMed principles for cybersecurity management; 3. Strengthen Coordinated Disclosure – need to have a process for researchers and others to disclose vulnerabilities; 4. Information Sharing, citing the value of sharing vulnerabilities for the benefit of the broader community; 5. Agree on consensus around standards and education, calling for consensus standards across the industry for healthcare cybersecurity. He commended the FDA for their leadership and relationship with the manufacturers.

Terry Rice said that cybersecurity vulnerabilities are more acute in the healthcare industry. He made 5 points: 1. The number of cybersecurity incidences are under reported; 2. More breaches occur than are reported; 3. The diversity of the healthcare industry means that many small and midsize organizations have no resources for cybersecurity; 4. The need for data portability poses an increased risk; 5. Advances in technology and electronic health records (EHRs) will open the industry to a wide array of threats. He also made 5 recommendations: 1. Ensure a senior official at HHS is in charge of cybersecurity to serve as a liaison to the private sector; 2. Work with the SCC on a comprehensive cybersecurity protection plan; 3. Improve the quality of intelligence shared among the NH-ISAC, HHS and the Department of Homeland Security; 4. HHS, SCC, NH-ISAC should conduct tabletop exercises; 5. HHS, DHS, SCC should work with global agencies to share intelligence and best practices.

Congressman Murphy asked about the worst case scenarios if the industry continues to be hit by attacks. He also asked why the NH-ISAC isn’t on par with other ISACs.

Congresswoman DeGette asked if a medical device has actually been taken over. Mr. McNeil said, to his knowledge, only in demonstration scenarios. She asked if risks are to single devices or classes of devices. Mr. McNeil said potentially classes of devices. She has what more can be

done to advance the NH-ISAC. Ms. Anderson said that awareness needs to improve about the ISAC and potentially pursue tax breaks or other incentives to grow participate. Congresswoman DeGette cited the grant funding awarded from HHS to the NH-ISAC, asking what else is necessary. Ms. Anderson said ISAC participation should be built into the NIST Framework and senior-level management should partake in the ISAC. Mr. Rice mentioned that the Financial Services (FS)-ISAC has over 6,000 members, the NH-ISAC has 200, so the membership needs to grow.

Congressman Griffith asked about legal protections for information sharing. He suggested that if a vulnerability is shared, but not fixed by a medical device manufacturer, they should not hide behind any legal protections. Witnesses suggested that type of information isn't likely to be shared through an ISAC, but agreed that legal protects are complex. The witnesses also acknowledged that information has increased since the passage of the Cybersecurity Act of 2015.

Congresswoman Schakowsky cited an article describing persistent vulnerabilities in medical devices and a lack of evidence that the manufacturers are adequately securing these devices. Mr. McNeil said that manufacturers should follow the mantra of patient safety and need to acknowledge the lifecycle changes of devices. He suggested more risk assessments and testing in clinical environments as means to improve security of devices. She asked about how customers are alerted about vulnerabilities. Mr. McNeil said that communications are an area of focus in a security program and they communicate through the FDA.

Congressman Burgess asked why potential misuse of health data is not trigger notification in a similar fashion as when banks perceive unauthorized access. Ms. Anderson said that should and could happen. Dr. Burgess cited a ransomware incident at a healthcare organization in Austin in which it appears that all of the proper protocols where followed yet the organization was still fined and put on the Wall of Shame. He said that HITECH established the Wall of Shame and that potentially Congress should revisit its usefulness. Mr. Rice suggested a case-by-case approach be taken on the Wall of Shame, he suggested a National Transportation Safety Board (NTSB) model for disclosures.

Congresswoman Clarke asked what is being done to prevent breaches and how the NH-ISAC is bringing small companies into the fold. The witnesses said the membership needs to grow and capabilities need to be expanded, and additional resources should be introduced into the public domain to help smaller organizations.

Congresswoman Brooks referenced the letter sent with Congresswoman DeGette to the FDA on device security. She asked how the FDA has worked with the industry. Mr. McNeil said the FDA has done workshops and conducted outreach to bring the fragmented pieces of the industry to the conversation. He cited the pre-and post- market guidance as examples of the FDA accelerating the industry's focus on cybersecurity. Congresswoman Brooks cited the multiple agencies in HHS that have cybersecurity roles and the brief 2-page cybersecurity strategy. Mr. Rice said they need to expand the cybersecurity plan.

Congressman Collins questioned the value and cost for small entrepreneurs to participate in the NH-ISAC. Ms. Anderson told him the lowest membership cost is $1,200/year, which Congressman Collins said was too much for small innovations. Congressman Collins also said that he believes congress should revisit the Wall of Shame, especially to get off the wall.

Congressman Ruiz asked about the value proposition of the NH-ISAC, the HHS Cybersecurity Taskforce and the severe shortage of qualified security professionals. The witnesses said that the education system is key, cybersecurity should be built into computer science programs.

Congresswoman Walters asked what actions HHS should take. The witnesses said HHS should make it clear that best practice is to join the NH-ISAC and they should establish a senior official to handle cybersecurity. Mr. McNeil said that HHS should encourage transparency in medical devices, included a software bill of materials to offer greater visibility of software needs. Mr. Rice asked that implementation guidance be developed for the NIST Cybersecurity Framework for small entities, he echoed the need for a software bill of materials. Mr. McNeil also answered a follow-up question about the need for a med-CERT similar to US-CERT for healthcare specific needs. The witnesses agreed that information sharing should be encouraged.

Congressman Costello asked what barriers to entry are entities to participate in the NH-ISAC. Ms. Anderson said that the NH-ISAC is running a free trial program, and money is always a factor in participation.

Congressman Carter referenced an effort in Georgia to expand the cybersecurity workforce. He also asked about examples of successful collaboration. The witnesses cited the NH-ISAC, FDA and MDISS relationship.

Congressman Murphy closed the hearing saying that they subcommittee will continue to pursue these issues. He mentioned opportunities for simplification and the need for different departments to work together.