Health Care Industry Cybersecurity (HCIC) Task Force Meeting

Meeting Information

Date: Thursday, April 21, 2016, 8:30am to 12:00 pm
Location: United States Access Board, 1331 F Street, NW, Washington, DC 20004

Key Highlights

- Received opening remarks from Mary K. Wakefield – Acting Deputy Secretary, U.S. Department of Health and Human Services HHS).
- Gained increased insight into programs in place at the Department of Homeland Security (DHS), the progress of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and received briefings from the Energy and Finance sectors regarding current initiatives and best practices.

Discussion Summary

Welcome and Introductions

Mary Wakefield, Acting Deputy Secretary, HHS

Mr. Emery Csulak welcomed attendees to the first public meeting of the HCIC Task Force and introduced Acting Deputy Secretary Mary K. Wakefield. Acting Deputy Secretary Wakefield commented on the changes within the health care industry over the last several decades, noting the transition from paper charts to electronic health records, interconnection of disparate hospitals and health care organizations, and increase in health care coverage across the Nation. She continued that the evolution of technology will continue to reshape the health care sector and that the protection of patient information must continue to evolve with technological advancements, as privacy and security are the bedrock of a successful health care system. She stated that the work of the Task Force will allow individuals to privately communicate with their physician and for clinicians to have access to a wide array of patient data without endangering the individual. She thanked HCIC Task Force members for serving on and contributing their varying skills and experiences. Acting Deputy Secretary Wakefield concluded by thanking the Task Force and stating that she looked forward to hearing about their future accomplishments.

Health Care Industry Cybersecurity Task Force Overview

Emery Csulak, Chief Information Security Officer (CISO), Centers for Medicare & Medicaid Services and Task Force Co Chair
Theresa Meadows, Senior Vice President and Chief Information Officer (CIO), Cook Children's Health Care System and HCIC Task Force Co Chair

Mr. Csulak introduced himself and reviewed the objectives of the HCIC Task Force. He specified that the goal of the Task Force was to address cybersecurity issues that are unique to the health care industry, not to develop new regulations, and that the day's session would help to identify and document best practices and lessons learned from other critical infrastructure sectors that could also help the health care sector improve its security posture. Mr. Csulak reviewed the responsibilities of the Task Force under the *Cybersecurity Information Sharing Act of 2015* (CISA) and added that the Task Force planned to hold three additional public meetings.

Ms. Theresa Meadows thanked participants and expressed her gratitude to represent the private sector on such a critical topic. She stated that the work of the Task Force will provide her organization and other providers with increased safety practices and allow for the sharing of critical information. She added that the efforts of the HCIC Task Force will allow for the development of a framework that will serve to protect both organizations and patients. Ms. Meadows concluded by stating that the Task Force is composed of a cross sector of the health care industry and that the diverse membership will promote robust dialog.

DHS/NIST Cross Sector Overview

Laura Laybourn, Director, Stakeholder Engagement and Cyber Infrastructure Resilience, Office of Cybersecurity and Communications, DHS and HCIC Task Force Member
Matthew Barrett, Program Manager, Cybersecurity Framework, NIST

Ms. Laura Laybourn provided an overview of DHS' cybersecurity vision and mission. She stated that the Department focuses on critical infrastructure and the promotion of best practices, information sharing, and incident response in order to help the public and private sectors to manage and improve their risk posture. Ms. Laybourn highlighted the National Cybersecurity and Communications Integration Center (NCCIC) as the nation's 24/7 cyber situational awareness and management hub in support of exchange with civilian government, state/local/tribal/territorial, private sector, and international entities.

Ms. Laybourn outlined the role and allocation of Sector Specific Agencies (SSAs) and discussed the Communications Sector as an example of how industry and government collaborate on policy, planning, and operations activity. She explained DHS' information sharing resources to include the Automated Indicator Sharing, Cyber Information Sharing and Collaboration Program, Enhanced Cybersecurity Services, and Information Sharing and Analysis Centers/Organizations. She provided overviews of the Critical Infrastructure Cyber Community Voluntary Program (C^3VP), which serves as the best practices promotion arm of DHS, and several of the voluntary cybersecurity evaluation resources offered by DHS.

Ms. Laybourn reviewed the concept (protect/perform and sustain/repeat) of cyber resilience and noted the 10 cyber resilience domains of DHS' no cost Cyber Resilience Review (CRR) that measures cyber security capabilities of an entity during normal operations and times of operational stress. She highlighted several of the CRR domains that are mapped to the NIST framework, ranging from i) 'asset management' as the cornerstone of the assessment and an inventory of people, information, technology and facilities; ii) 'external dependency management' focused on supply chain/third parties that requires collaboration among diverse groups of internal organizational stakeholders and typically results as an underperforming practice area; and iii) 'service continuity management' as a domain of particular importance to the health care sector.

Mr. Matthew Barrett provided an overview of the NIST Cybersecurity Framework. He stated that NIST has collected anecdotal evidence and a common taxonomy for cyber outcomes. He continued that the framework includes a methodology to measure cyber risk management practices in the form of implementation tiers and includes a tool to dynamically reprioritize cybersecurity efforts. Mr. Bennett added that NIST is contemplating a minor update to the framework based on industry feedback requesting additional refinements and clarification.

Mr. Barrett reviewed the patterns of use and to adopt the framework, which first includes trying to understand and evaluate the framework, then making a decision about whether to implement the framework. He noted that individuals use the Framework to determine where an organization currently

operates, identify the desired future state, and understand the activities required to allow them to achieve their end goal. He also reviewed the Framework categories, subcategories, crosswalks, and associated profiles that can assist individuals at all levels of technical expertise. He also highlighted the requests for information (RFI), which are available on the NIST website, and recommended that participants review the RFI responses. Mr. Barrett emphasized the voluntary nature of the framework and concluded by stating that NIST looks forward to engaging the health care and public health sectors to implement the Cybersecurity Framework.

Cybersecurity Best Practices – Energy Sector Panel

Mike Smith, Senior Cyber Policy Advisor, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy (DOE)
Fowad Muneer, Program Manager, Office of Electricity Delivery and Energy Reliability, DOE
Nadya Bartol, Vice President, Industry Affairs and Security Strategist, Utilities Telecom Council

Mr. Mike Smith provided opening comments and explained that the vast majority of his office's funding and investment for research and development focuses on industrial control systems. As a Federal Agency, the office cannot fund activities that compete with the private sector and, therefore, the office seeks to identify gaps and invest funding in areas where organizations do not have the resources, finances, or time to develop these processes and guidance documents.

Mr. Fowad Muneer discussed the roles and responsibilities for providing critical infrastructure security and reviewed the office's function to serve as the point of contact for collaboration with private industry. He added that the office works in coordination with national laboratories, private sector partners, and interagency partners to provide technical assistance for incidents. Mr. Muneer reviewed the purpose and goals of the Sector Coordinating Council (SCC) and noted that the sector developed a voluntary roadmap in 2006 (revised in 2011) for cyber delivery systems to ensure that "the lights stayed on." The ultimate vision is to create resilient energy systems that survive cyber incidents while sustaining critical functions. He added that the office works in collaboration with industry to increase the adoption of existing best practices and standards, as well as to bring required services and capabilities to affected parties at the right time.

Mr. Muneer reviewed several examples of collaboration between DOE and sector members to include the Cybersecurity Capability Maturity Model (C2M2). C2M2 serves as a maturity model that was developed in collaboration with 200 industry experts and includes a maturity scale to measure the institutionalization of security practices. Mr. Muneer concluded by saying that since its development, approximately 750 organizations from a variety of sectors have requested a C2M2 evaluation and stated that all programs are available and free to use via the Office of Electricity Delivery & Energy Reliability website.

Ms. Nadya Bartol provided an overview of the Utilities Telecom Council, energy sector, standards, and regulatory bodies that play a role in the sector's functioning and operations. She discussed the relationship between energy and cybersecurity and added that the sector is diverse in terms of the implemented cybersecurity processes and practices. Ms. Bartol stated that at its inception, the energy sector was not intended to be connected to the internet. However, the connection of the energy sector to business networks created unintended threats and resulted in the need for increased cybersecurity. She added that within the sector, there is a lack of cybersecurity expertise and that by 2020 the sector will need to fill approximately 1.5 million cybersecurity positions.

Ms. Bartol reviewed the regulatory environment for the energy sector, specifically initiatives from the North American Electric Reliability Corporation and Federal Energy Regulatory Commission. She also

explained the difficulty in implementing security guidelines due to the specificity of the requirements. One solution is to make the higher level requirements for easier implementation. She stated that the importance lies in creating the right level of specificity so that requirements can be both easily understood and implemented, but not so broad that individuals could not deploy the requirement. Ms. Bartol concluded by confirming the value of the C2M2 tool to organizations within the energy sector.

Cybersecurity Best Practices – Banking and Finance Sector Panel

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

Mr. Brian Peretti began by expressing his interest in sharing information with the healthcare sector and noted the alignment between health care and financial services due to commonalities in the insurance businesses of both sectors. He explained that the Office of Critical Infrastructure Protection and Compliance Policy was established following 9/11 as individuals did not understand the operational risks that were uncovered as a result of the attacks. Mr. Peretti emphasized the need for information sharing because banking and finance functions utilize the infrastructure of other critical infrastructure sectors. He continued that cybersecurity underlies modern society and identified three key aspects and practices to assist in preventing and managing these issues:

- **Comprehensive Information Sharing**: To conduct risk management and manage risks appropriately, organizations need the highest quality information available. The more insight an organization has to the systems within its enterprise, the better the feedback the organization will receive related to inherent risks.
- **Baseline Protections**: Organizations can take multiple steps to increase the security of their infrastructure to include patching against known vulnerabilities, deploying industry accepted best practices, and understanding how those practices protect systems. Implementation of baseline protections is increasingly required by consumers who refuse to do business with entities that do not protect their assets. To promote baseline protections, industry needs to communicate information in a way that is understandable to the consumer and prompts organizations to take decisive actions to implement the baselines.
- **Response and Recovery**: Even with quality information and baseline protections in place, incidents will still occur. The office is currently collaborating with the private sector to develop these processes and get systems back online. Critical to response and recovery efforts is developing and engaging in testing and exercising response activities to understand how the organization will identify and react to incidents. The office also developed a program in collaboration with Government and industry to identify challenges and risks, as well as developed an all hazards playbook for organizational use.

Mr. John Carlson began by stating that the finance sector has established efforts coordinating with Government partners (e.g., DHS, NSA, law enforcement) and noted that this type of engagement is beneficial to promote engagement and awareness within the private sector. He described the five areas that contribute to cybersecurity resilience:

- Increasing information sharing and improving threat analysis;
- Identifying additional controls that support cybersecurity efforts;
- Enhancing the ability to respond during a crisis through established mechanisms and trusted sources to assist in response efforts;

- Enhancing the ecosystem by sharing threat information and enhancing communications; and
- Creating education and advocacy to promote information sharing and to protect the information organizations do share.

Mr. Carlson provided an overview of the Financial Services Information Sharing and Analysis Center (FSISAC) and reviewed the Circles of Trust and Traffic Light Protocol, which support FSISAC members in the event of an incident and also place controls on the sharing of certain information. He also reviewed the information sharing tools available to the FSISAC and highlighted Soltra and the Hamilton series of exercises. Mr. Carlson added that as a result of these exercises, the electric and communications sectors have increased their resiliency due to the known interdependencies of the two sectors. He reviewed the investments the ISAC has made to protect the sector, the Financial Services SCC mission, and the 2016 priorities for the financial sector. Mr. Carlson concluded by noting the effort the ISAC is promoting industry engagement and awareness at the executive level, advancing cross sector collaboration, and developing tactical level playbooks for response efforts and to continue to educate policy makers.

Closing Remarks

Emery Csulak, CISO, CMS
Theresa Meadows, Senior Vice President and CIO, Cook Children's Health Care System

Mr. Csulak provided attendees with a high level overview of the HCIC Task Force expectations and stated that the Task Force would continue to communicate with the public on its progress. He added that future public meetings are tentatively scheduled to occur on July 21, September 15, and December 15, 2016. Mr. Csulak thanked the speakers, Task Force members, and public participants and ended the open session of the HCIC Task Force Meeting.

Attendees

Table 1 List of Attendees of the open session of the HCIC Task Force Meeting.

LAST NAME	FIRST NAME	ORGANIZATION
Allen	Arthur	Politico
Amato	Maggie	HHS
Barrett	Matthew	NIST
Bartol	Nadya	Utilities Telecom Council
Brice	Ebony	ONC/OCPO
Buchholz	Benjamin	Department of Justice
Carlson	John	FSISAC
Centola	Joanna	Deloitte
Corman	Joshua	I Am The Cavalry
Coughlin	Jeff	HIMSS
Cressey	Roger	Liberty Group Ventures
Csulak	Emery	CMS
Curren	Steve	HHS – ASPR
Dean	Danielle	National Conference of State Legislatures
DeCarlo	Michael	Blue Cross Blue Shield Association
DeCesare	George	Kaiser Permanente Health Plan
Edison	Nicole	HHS – APSR
Fassl	John	U.S. Department of the Treasury
Fernando	Anura	UL, LLC
Finn	David	Symantec
Fraser	Stephanie	Deloitte
Gleason	Joe	AHT Insurance
Gray	David	HIMSS
Jarrett	Mark	Northwell Health/Hofstra Northwell School of Medicine
Johnson	Alissa	Stryker Corp.
Kempton	John	AHT Insurance
Krigstein	Leslie	CHIME
Laybourn	Laura	DHS
Leitsch	Darren	Deloitte
Marsh	William	Defense Healthcare Management Systems
McNeil	Michael	Philips Healthcare
McWhorter	Dan	FireEye
Meadows	Theresa	Cook Children's Health Care System
Mellinger	Roy	Anthem

LAST NAME	FIRST NAME	ORGANIZATION
Mendelson	Tina	Deloitte
Monahan	Kenneth	HHS/ASPR/OEM/CIP
Monson	Jacki	Sutter Health
Muneer	Fowad	DOE
Peretti	Brian	U.S. Department of the Treasury
Ramadoss	Ram	Catholic Health Initiatives
Rice	Terry	Merck & Co.
Robbins	Kristin	Deloitte
Ross	Aftin	Food & Drug Administration
Salmogl	Gene	U.S. Department of Treasury
Sardanopoli	Vito	Quest Diagnostics
Savickis	Mari	CHIME
Shields Uehling	Mary (Mollie)	SAFE BioPharma Association
Smith	Mike	DOE
Struse	Richard	DHS
Suarez	Walter	Kaiser Permanente
Sublett	Christine	Augmedix
Thompson	Lauren	Department of Defense/Department of Veteran Affairs
Ting	David	Imprivata
Todt	Kiersten	NIST
Trotter	Fred	CareSet Systems
Trumpoldt	Ken	Deloitte
Wakefield	Mary	HHS
Weber	Rick	Inside Cybersecurity
Wolf	Laura	HHS
Zuk	Margie	The MITRE Corporation