Testimony of

Denise Anderson

On Behalf of the

The Health Information Sharing & Analysis Center (Health-ISAC)

and the

Health Sector Coordinating Council Cybersecurity Working Group

Before the

United States Senate

Committee on Health, Education, Labor, and Pensions

May 18, 2022

ISAC Background

Chair Murray, Ranking Member Burr, and members of the Committee, my name is Denise Anderson. I am President and CEO of the Health Information Sharing & Analysis Center (Health-ISAC), Chair of the National Council of ISACs (NCI) and serve on the Executive Committee of the Health Sector Coordinating Council Cybersecurity Working Group (HSCC CWG). I want to thank you for this opportunity to address the Committee on Health, Education, Labor, and Pensions about the industry perspective on cybersecurity threats to the Health sector and the resulting challenges and impacts, as well as the activities the sector is undertaking to combat these threats including collaborating and coordinating within, between and across the public and private critical infrastructure sectors.

ISACs were formed in response to the 1998 Presidential Decision Directive 63 (PDD 63), which called for the public and private sectors to work together to address cyber threats to the nation's critical infrastructures. After 9/11, in response to Homeland Security Presidential Directive 7 (its 2013 successor, Presidential Policy Directive 21) and the Homeland Security Act, ISACs expanded their role to encompass physical threats to their respective sectors. Many ISACs have been in existence over a decade and in some cases over two decades.

ISACs are industry driven, trusted communities that promote the sharing of timely, actionable, and reliable information for their respective critical infrastructure sectors and provide forums for owner and operator sharing around threats, incidents, vulnerabilities, best practices, and mitigation strategies. ISACs are operational in nature and have strong reach into their sectors to gather and disseminate information quickly and efficiently. ISACs have been thriving and growing in recent years as owners and operators have seen the benefit to participating in these trusted communities, which is a testament to the value ISACs deliver to their members. ISACs coordinate with each other through the National Council of ISACs (NCI), a voluntary organization formed in 2003.

HEALTH-ISAC BACKGROUND

Health-ISAC, (www.h-isac.org) founded in 2010, is a 501(c)6 nonprofit organization and is funded primarily by its member firms through member dues. Since 2010 the membership has expanded to over 700 organizations including healthcare delivery organizations (HDOs), providers, academic medical centers, medical research and development centers, medical materials manufacturers and distributors, pharmaceutical and medical device manufacturers, retail pharmacies, laboratories and radiological centers, telehealth providers, electronic health record providers and payers representing approximately two-thirds of the US Health and Public Health GDP*.

Health-ISAC members represent 79 percent of the top 103 hospital chains in the United States, 61 percent of the top 51 global medical device manufacturers, 84 percent of the top 25 global pharmaceutical manufacturers, 93 percent of Fortune 500 healthcare companies in the United States and 86 percent of electronic health record providers in the United States. Our members range from small organizations with less than one million dollars in annual revenue to large Fortune 50 organizations with over 238 billion dollars in annual revenue.

*Based on the annual revenue of all Health-ISAC member organizations. ($2.3 Trillion).

Health-ISAC is a global organization that has members headquartered in over 20 countries and membership is growing rapidly. Health-ISAC saw its largest member growth ever in 2021.

The mission of Health-ISAC is to empower trusted relationships in the global healthcare industry to prevent, detect and respond to cyber- and physical security events so that members can focus on improving health and saving lives.

Besides offering a trusted forum and community for sharing information around threats, vulnerabilities, best practices and mitigation strategies, Health-ISAC offers a number of other services such as global workshops and webinars, four annual summits – two in the United States, one in Europe and one in Asia, daily cyber and physical reports, alerts, targeted threat alerts, a monthly newsletter, a weekly blog on cybersecurity issues in healthcare, white papers, monthly member-only threat briefings, monthly podcasts, exercises, special interest groups, a number of working groups and committees and various technical tools and partner programs for members to use in their environments. In addition, the Health-ISAC Threat Intelligence Committee (TIC) sets the sector cyber threat level monthly, or as needed, and provides valuable insight and mitigation strategies when threats arise, or incidents occur.

Health-ISAC has numerous sharing and collaboration channels, including platforms where hundreds of thousands of actionable indicators and threat actor tactics, techniques, and procedures (TTPs) are shared. Health-ISAC was one of the first organizations to adopt STIX and TAXII, which are protocols for automated indicator and intelligence sharing and fosters a robust member machine-to-machine sharing environment. Health-ISAC uses the Traffic Light Protocol, (TLP) an information owner dissemination determination protocol for sharing of information. TLP RED is the most restricted sharing protocol, with TLP WHITE, the broadest. Over 100,000 individuals have access to our TLP GREEN and TLP WHITE alerts.

In 2021, for example, Health-ISAC:

- Provided alerts, papers, webinars, thought leadership and facilitated collaboration on myriad incidents during the year including SolarWinds, Accelion, ProxyLogon, PrintNightmare, VPN Vulnerabilities, in Fortinet, Pulse and Citrix, Colonial Pipeline, JBS Meats, Irish National Health Service, Kaseya, Geopolitical Tensions, Hurricane Ida and other physical threats, and Log4j.
- Added 119 new members amounting to a member community of over 5,500 individuals.
- Nearly tripled the number of member organizations using automated indicator sharing.
- Conducted twelve highly attended *Monthly Member Threat Briefings,* published 242 *Finished Intelligence Reports*, sent over 419 *Targeted Alerts,* held ten *Threat Operations Center* (*TOC) Spotlight* threat and vulnerability webinars, and distributed over 65,812 actionable indicators of compromise.
- Worked with security researchers to develop four pre-public alerts and vulnerability notifications impacting millions of medical devices.
- Stood up several new programs including a new webinar program, *Continue the Conversation* for members to bring subject matter expert panels and discussions around hot topics from the chat channels, the Microsoft Patch Tuesday Podcast and TOC Open House Office Hours.

- Hosted an Analytics Training Workshop, offered 63 webinars, and held three successful global in-person Summits, with our Fall Summit attendance close to pre-pandemic numbers. Health-ISAC also conducted nine customized exercises and in 2022 published an After-Action report from our 2021 *Rethinking Resiliency* exercise series.
- Planned, and held the Hobby Exercise, a tabletop exercise designed to engage the Health sector and strategic partners, including those in government, on significant security and resilience challenges. The overarching objective is to inform and provide opportunities for continuous organizational improvement while increasing Health sector resiliency. The annual exercise is named for Oveta Culp Hobby, the first U.S. Secretary of Health, Education and Welfare. The 2021 After-Action Report illustrating findings from the exercise was recently published in March of 2022.
- Worked with Cisco to conduct a well-received 2-day Leadership Development Course for rising CISOs at the 2021 Fall Summit. This was also held at our Spring Summit in May of 2022.
- Produced four whitepapers, developed Pharmaceutical and Supply Chain Guidance for practitioners and healthcare CISOs, and expanded physical threat information deliverables for Health sector organizations. Also published *Full* and *Lite* versions of copyrighted *Health-ISAC Questionnaires* for Third-Party Risk Management. In 2022 we also published a whitepaper on *Securing the Modern Pharmaceutical Supply Chain*.
- Offered valuable tools for members such as third-party risk management, digital risk protection and internet traffic visualization through our Community Services Program.
- Facilitated five Committees, over 15 Working Groups and three Councils devoted to topics such as Cybersecurity Analytics, Information Security Incident Response, Security

Engineering and Architecture, Business Resiliency and Cybersecurity Awareness and Training.

- Continued to build on our work to improve security across the Medical Device Community with over 25 medical device public advisories, two Food and Drug Administration (FDA) Town Halls at Health-ISAC Summits and curated medical device information related to Log4j and other vulnerabilities on the Health-ISAC website. Our Medical Device Cybersecurity Information Sharing Council is comprised of 331 individuals from 135 organizations with half of the group comprised of Healthcare Delivery Organizations (HDOs) and the other half comprised of Medical Device Manufacturers (MDMs).
- Conducted over 30-member interest surveys on topics such as SolarWinds Impact, Security Workforce Size and Strategy, and Security Operations Centers Resourcing.

In 2022, to date, Health-ISAC has engaged in five major activities of note. The first is the publishing of the first annual Health-ISAC report on the *Current and Emerging Healthcare Cyber Threat Landscape* in both TLP GREEN and TLP WHITE versions. The report features survey results on member threat perspectives, as well as, top issues from 2021 and a look ahead into 2022 (*https://h-isac.org/health-isacs-first-annual-current-and-emerging-healthcare-cyber-threat-landscape-executive-summary/*). The second is the publishing of the 2021 Health-ISAC Annual Report (*https://h-isac.org/2021-annual-report/*). Third, the ISAC held several webinars, produced alerts and briefings, and published a joint bulletin with the Health Sector Cybersecurity Coordination Center (HC3), part of the Department of Health and Human Services (HHS), regarding the geopolitical tensions in Russia. The ISAC emphasized several messages to the sector that resulted from Classified briefings conducted by the White House, Cybersecurity and Infrastructure Security Agency (CISA), and its partners and stood up a working group of members directly impacted by the situation so that they could share challenges, issues, and best practices with each other. Fourth, Health-ISAC worked on another pre-public vulnerability disclosure with CISA and CyberMDX/Forescout on Access: 7 vulnerabilities found in PTC Axeda agenda and Axeda Desktop server.

Fifth, in April 2022, Health-ISAC worked with Microsoft and others to take down the Zloader malware family, one of the most notorious cybercrime operations responsible for ransomware attacks against hospitals in the United States and around the world. The takedown was accomplished through coordinated legal and technical actions and disrupted massive botnets using the Zloader malware family, striking a major blow against cybercriminal operators using Ransomware, such as Ryuk, to extort victims.

With the seizing of hundreds of domain names used by the Zloader malware to remotely command and control victim computers, Microsoft will use the intelligence gained from this takedown to partner with Law Enforcement, Internet Service Providers and Computer Emergency Response Teams around the world to help remediate infected computers, making the Internet safer for consumers and businesses worldwide. Together, these aspects of the operation are expected to undermine the criminal infrastructure that relies on these botnets every day to make money and helps to provide new tools for the industry to work together to proactively fight cybercrime.

At Health-ISAC, our mission is much bigger than the ISAC. We believe building a stronger community both inside and outside of the sector leads to better patient care and a healthier world.

HEALTH SECTOR COORDINATING COUNCIL CYBERSECURITY WORKING GROUP

BACKGROUND

Healthcare is designated under U.S. national policy as "critical infrastructure" along with 15 other industry sectors, such as financial services, energy, telecommunications, water, transportation and more, represented by industry-organized "Sector Coordinating Councils (SCCs)." These SCC's and their government counterparts form a national public-private partnership coordinated overall by the U.S. Department of Homeland Security through the National Infrastructure Protection Plan (NIPP). The Health Sector Coordinating Council (HSCC) serves as an official advisory council to its government counterparts - HHS and FDA – with a formally-designated critical infrastructure protection function distinct from the advocacy and member services roles of traditional industry associations. The HSCC, HHS and FDA work jointly to identify and mitigate systemic threats to critical healthcare infrastructure, such as pandemics, major weather events, terrorism, active shooters, and cyber-attacks, with a mission to identify cyber and physical risks to the security and resiliency of the sector, develop guidance and policies for mitigating those risks, and facilitate threat preparedness and incident response. The Office of the White House National Cyber Director has identified and engaged the HSCC as a model to accelerate a national healthcare cyber resilience strategy.

The HSCC Cybersecurity Working Group (CWG) is a volunteer coalition of 320 organizations that operate under a charter-based governance structure with an elected Chair, Vice-Chair and

Executive Committee. Membership is open to any organization that is a) covered entity or business associate under HIPAA; b) a Health plan or payer; c) regulated by FDA as medical device or pharmaceutical company; d) regulated by HHS Office of the National Coordinator as a Health IT company; e) a public health organization and f) a healthcare industry association or professional society. A small allotment of an "Advisor" member category of consulting and security companies is permitted to participate and support CWG initiatives pro-bono.

When working with our government partners, the industry-led Cybersecurity Working Group becomes the *Joint* Cybersecurity Working Group, which identifies and develops preparedness measures against cybersecurity threats to the security and resiliency of the Health sector. It is organized into outcome-oriented task groups (currently 13) that meet regularly to develop best-practices for various healthcare cybersecurity disciplines such as 405(d) Health Industry Cybersecurity Practices, Supply Chain Cyber Risk Management, Five-Year Plan, Emerging Technology, Workforce Development, Measurement, Policy, Outreach and Awareness and Risk Assessment and Medical Technology Security including sub-groups around the Joint Security Plan Update, MedTech Legacy Devices, and MedTech Vulnerability Communications.

The CWG has produced 15 major best-practices publications since 2019, freely available to sector stakeholders and the public via its website (*HealthSectorCouncil.org*). These publications include *Health Industry Cybersecurity Practices, Health Industry Cybersecurity Tactical Crisis Response Guide, Health Industry Cybersecurity Securing Telehealth and Telemedicine, Model Contract Language for Medtech Cybersecurity Medtech Vulnerability Communications Toolkit* and *Operational Continuity Cyber Incident*.

Many of these HSCC CWG task group initiatives and deliverables directly address the many important recommendations contained in the 2017 HHS report of the Health Care Industry Cybersecurity (HCIC) Task Force, which was established by the Congress in Section 405(c) of the 2015 Cybersecurity Information Sharing Act and was composed of industry and government experts in healthcare and cybersecurity. At the time, the report characterized the healthcare industry's cybersecurity preparedness as being "in critical condition." As the Health Sector Coordinating Council has been focused on developing cybersecurity best practices and tool kits – by the sector, for the sector – we hope that as more healthcare organizations implement these scalable practices over time, we will raise the sector's preparedness diagnosis to "stable." But in the business of cybersecurity, we are never done, only better.

To support the development of these initiatives, our preparedness, information sharing and incident response, both Health-ISAC and the HSCC CWG work closely with HHS and FDA, both of which serve as our CWG co-chairs and Sector Risk Management Agency (SRMA), as well as, CISA. Our ongoing partnership engagement includes holding weekly calls with the leadership in each organization to assess and discuss issues facing the sector.

THE CYBER THREAT LANDSCAPE IN HEALTHCARE

Ten years ago, 'cyber' and 'healthcare' were not even placed in the same sentence. Today because of the rise in digital healthcare, the proliferation of advances in technology and the efficiencies of connecting devices and data, the cyber threat surface in healthcare has ballooned and the threat actors have followed. Threat actors have many motivations to attack whether for financial reasons, disruption, intellectual property theft, revenge or to make a political statement.

Unfortunately, the stakes are very high. The focus has traditionally been on data and privacy but if HDOs, providers, or their suppliers cannot deliver services, as was seen in numerous ransomware attacks, or data is manipulated or destroyed, patient lives can be at risk.

There are essentially five malicious actor groups that are responsible for threats to healthcare, which include Nation States such as Russia and China, Cyber Criminals, Hacktivists, Terrorists, and Insiders who can be malicious or non-malicious. Their motivations range from **Advantage** – intellectual property theft, gain a foothold for further disruption, espionage, blackmail – **Ego** – notoriety, revenge – **Ideology** – political, social, cultural and **Greed** – money, power.

The various actor groups use several Tactics, Techniques and Procedures (TTPs) to conduct their activity. Some TTPs are Phishing and Spearphishing, Ransomware, Wipers, Distributed Denial of Service (DDoS), Business Email Compromise, Remote Access, Supply Chain Attacks, Scanning and Exploiting Vulnerabilities, Social Engineering and Credential Theft.

In November 2021, Health-ISAC conducted a survey of its members asking them to rank order the Top 5 "*greatest cybersecurity concerns*" facing their organizations for both 2021 and 2022. The survey included cyber (e.g., CISO) and non-cyber executives (e.g., CFO), multiple healthcare subsectors (e.g., Providers, Pharmaceutical Manufacturers, Payers, Medical Device Manufacturers, Health Information Technology), as well as, healthcare organizations of varying sizes and budgets. The Top 5 threats, which were the same for both 2021 and 2022 were:

1. Ransomware Deployment
2. Phishing/Spear-Phishing Attacks

3. Third-Party/Partner Breach
4. Data Breach
5. Insider Threat

Ransomware has had a big impact on the Health sector and threat actors have evolved their techniques over the last two years from simply just asking for a payment to unlock files to blackmailing organizations with threats to release records to the public. According to the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center's (IC3) 2021 *Internet Crime Report*, the Health sector experienced at least 148 ransomware attacks between June of 2021 and December of 2021 resulting in millions of dollars of losses.

Ransomware family groups that have been particularly prolific in the healthcare sector include Conti and its Ryuk Ransomware. Ryuk has been linked to more than 200 ransomware attacks impacting hospitals, public health departments, nursing homes and patient care facilities around the world since 2018. The attacks resulted in the temporary or permanent loss of IT systems that support many of the provider delivery functions in modern hospitals resulting in cancelled surgeries and delayed medical care. Some examples of impacts caused by Ryuk at patient care facilities in the United States since 2018 include:

- Ryuk attack forced ambulances to divert, causing a 90-minute delay in emergency patient services.
- Ryuk disrupted delivery of chemotherapy treatments for cancer patients.
- Ryuk forced hospitals to cancel elective procedures.

- Ryuk caused delays in reporting of laboratory results.
- Ryuk caused delays in scheduling appointments for maternity and oncology patients.
- Ryuk caused more than three weeks of downtime for the Electronic Health Records management system.
- Ryuk impacted systems at nursing homes, causing patient records to be unavailable and prohibiting pharmaceuticals orders from being placed, and
- Ryuk leaked sensitive patient data including treatments, diagnoses, and other information of hundreds of thousands of people.

Hospitals reported revenue losses due to Ryuk infections of nearly $100 million from data Health-ISAC obtained through interviews with hospital staff, public statements, and media articles. The Ryuk attacks also caused an estimated $500 million in costs to respond to the attacks – costs that include ransomware payments, digital forensic services, security improvements and upgrading impacted systems plus other expenses. A high-profile attack as the result of Conti/Ryuk was against the Health Service Executive (HSE), the national health system in Ireland consisting of 54 hospitals, in May of 2021. The attack brought all the IT systems within HSE nationwide down and it took four months to completely recover from the incident.

Other Ransomware families are REvil/Sodinokibi, Hive, Lokibot, Pysa and Clop. Health-ISAC assesses that in 2022, Ransomware will continue to proliferate, and cybercriminals will target critical systems to the operations of healthcare organizations to force healthcare organizations to pay a ransom quickly and not allow time for investigation or forensic examination prior to paying the ransom demanded.

The other impact of Ransomware is the downstream effects that result when suppliers are attacked. When Kronos, a Human Resources Management Solutions firm widely used in healthcare, was attacked in December of 2021, numerous hospitals were impacted. Hospitals were forced to manage payroll, staff scheduling, and issuing staff IDs manually during a surge in COVID-19 infections. In January 2021, when WestRock, a packaging solutions manufacturer that was essential in providing packaging for COVID-19 vaccines, treatments, and diagnostics, was hit with a Ransomware attack, pharmaceutical manufacturers were impacted by slowdowns in package production and shipping during a vital period in the pandemic.

The COVID-19 Pandemic was a factor in several incidents that took place over 2020 and 2021. Nation State activity has always been present in the sector, but it was especially visible during the COVID-19 pandemic with the desire to gain knowledge about vaccines, diagnostics and therapeutics related to COVID-19. Threat actors accessed documents covering the regulatory submission for Pfizer and BioNTech's COVID-19 vaccine candidate BNT162b2 at the European Medicines Agency (EMA) where the documents had been stored on EMA's servers. There were also several incidents such as when threat actors attacked and blocked access to an Italian COVID-19 vaccination booking system. Other activities targeted organizations offering cold storage and delivery processes for keeping vaccines at safe temperatures with phishing and spear-phishing campaigns.

A concerning threat actor trend has been the intention and ability to target IT providers, Managed Service Providers and Enterprise Management Software Systems to gain access to a larger group of victims. For example, in February of 2020, threat actors affiliated with Russia's SVR (foreign intelligence service) injected malicious code into an update for SolarWinds Orion, a network monitoring software used by several organizations including the U.S. Federal Government. The malicious code went undetected until December 2020 and infected over 18,000 machines through the supply chain. Other high profile supply chain compromises included Kaseya and Accenture. Likely heading into 2022 threat actors will evolve this tactic and focus on compromising cloud providers to gain access to the sensitive data and networks of multiple victims.

Vulnerabilities also posed a huge problem for the sector. According to a graph published by the National Institute of Standards and Technology (NIST), vulnerabilities increased for a fifth straight year with 18,378 reported in 2021. Of that number, 3,646 were considered high-risk. Of particular note were the PrintNightmare vulnerability, the Microsoft Exchange Proxy Shell Attack vulnerability, and the Apache Log4j vulnerability which had very broad implications across the sector.

In 2022 there has been increased focus on Nation State activity and related criminal cyber activity surrounding the geopolitical events occurring between Russia and Ukraine. Many fear a fall-out from Russian activities against Ukraine such as what occurred during the 2017 Petya/Not Petya attacks that impacted over 300 companies, many of which were large multi-national corporations, and cost over $10 billion. Recent reporting shows Russian threat actors attacked Viasat, a US provider of high-speed satellite broadband services, one hour before Russia invaded Ukraine. Thousands of satellite terminals were affected impacting myriad internet users in Europe as well as over 5,800 wind turbines producing electricity. Even if healthcare is not directly targeted, cascading impacts such as access to communications and electricity can be substantial. Health-ISAC assesses that threat actor cyber activities will continue to rise and evolve, and the sector needs to be ever vigilant, as well as, develop robust enterprise risk management and resiliency strategies.

THE UNIQUE NATURE OF HEALTHCARE

The Health sector is highly inter-connected. Unlike in other sectors, healthcare data must be portable. Sensitive patient information must move between various medical providers, pharmacies, diagnostic facilities, and payers to facilitate proper patient care and history, as well as, payment for those services. Many healthcare facilities such as hospitals operate in environments that are accessible to the public. Hospitals employ tens of thousands of medical devices, many using outdated operating systems, and many of which are connected to a network. These devices are made by a variety of manufacturers with various levels of security and patching protocols built in. Expensive equipment such as Magnetic Resonance Imaging (MRI) machines are not easily replaced and run on software that is no longer patched or supported. In addition, many of these devices run 24 hours a day, seven days a week, 365 days a year, so taking them offline for patching or other security needs is complicated.

When supply chains are tightened or non-existent for various reasons, or pandemics or natural or man-made regional disasters occur, stretched supplies and staff become an additional factor.

Coupled with a diverse base within the sector, a highly regulated environment, complex siloed departments, a lack of skilled cyber staff, a lack of cyber security situational awareness, a lack of knowledge and training for the medical staff as well as at the CEO and Board level, and lack of cyber security strategy including a risk management approach, the Health and Public Health sector faces enormous challenges.

MEETING THE CHALLENGE

Despite the numerous challenges, many organizations in the Health sector have taken great strides to make certain their environments are as protected and resilient as they can be. As can be seen by the contributions of the Health Sector Coordinating Council Cybersecurity Working Group and Health-ISAC, countless individuals dedicate numerous hours of their time to help ensure the sector is strong and secure. Both the HSCC CWG and Health ISAC have robust communities that thrive on collaboration in their mission. As is the tradition in medicine, members of these two organizations truly care about patient welfare and safety and the protection of the ecosystem that contributes to them. Members share best practices, indicators of compromise, mitigation strategies and other vital information to accomplish this. When the Petya/Not Petya attacks of 2017 took place, some 60 individuals of approximately 34 Health-ISAC member firms came together and within 48 hours, determined what the actual attack was, the attack vector, how it spread and how to stop it and the shared their findings not just within the sector but globally via the Health-ISAC website and alerts. The publications produced, webinars and workshops held, exercises conducted and TLP WHITE alerts are open to the sector and are free. In 2021, Health-ISAC delivered targeted alerts to 49 healthcare companies that were non-members. The Zloader takedown will benefit countless organizations inside and outside of the sector and industry is looking to do more in this space.

Despite the number of great initiatives and efforts underway within the sector, the sector needs to be vigilant. We can no longer look at the challenges through just a cyber- or physical security lens, but must employ enterprise risk management to consider all threats to operational resilience. As evidenced by Hurricane Maria in Puerto Rico and its impact on the availability of IV bags, ransomware attacks on healthcare and healthcare suppliers, which have crippled healthcare delivery, the COVID-19 shutdown in Shanghai that has tightened the supply of contrast fluid used for imaging, which has forced physicians to prioritize which patients can get CT scans, MRIs and more, healthcare organizations must constantly be focused on all threats to healthcare delivery and patient safety. The healthcare sector should be supported and incentivized in this vital effort.

Congress can help meet this challenge by focusing on three key areas:

1-EDUCATION, RECOGNITION AND FACILITATION OF THE IMPORTANCE OF INFORMATION SHARING

One of the greatest challenges for Health-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 and SCCs exist and have valuable tools available to improve security – many of which are free to use. Numerous incidents have shown that effective information sharing amongst robust trusted networks of members works in combatting cyber threats.

Government, and specifically the SRMAs should regularly and consistently encourage owner/operators and especially at the Board and CEO level to join their respective ISACs and

Sector Coordinating Councils. 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.

The SRMAs indeed have a policy reference for this kind of advisory to their sector representatives: the NIST Cybersecurity Framework. This Framework, developed over the course of a year collaboratively by government and private sector stakeholders, lays out a cyber risk management framework linked to five core functions: identify, protect, detect, respond, and recover. Among the functional categories identified as part of a mature cyber risk management strategy is external communications and coordination around cyber security threats, response, and best practices. In other words, membership in an ISAC or ISAO and/or the SCC is an essential element of a successful cyber risk management strategy.

Another way to facilitate sharing and build robust communities is by providing financial incentives through tax breaks or other means to critical infrastructure organizations that join their respective ISACs and/or SCCs.

2-PROVIDE INCENTIVES FOR ADOPTION OF CYBERSECURITY BEST PRACTICES

Cyber threat actors are agile, in many cases run their operations as businesses, are sophisticated and constantly evolve their TTPs to infiltrate an organization’s defenses and achieve their goal. It is much easier to attack versus defend and healthcare organizations are often at a disadvantage, especially smaller organizations that do not have financial and infrastructure resources. Due to the huge growth in cybercrime and large ransomware payouts, sophisticated and organized criminal groups will be able to invest heavily into R&D and develop new ways to conduct automated and effective scams. The criminals will leverage machine learning, artificial intelligence, and deep fakes to perpetrate efficient and effective criminal campaigns. Therefore, it is essential to support healthcare organizations by incentivizing them to adopt at a minimum basic cybersecurity and risk management strategies. Some good best practices include employing multi-factor authentication (MFA) and other access controls, having a layered defense, using endpoint security, developing network segmentation, building prevention and detection strategies, backing up data and training staff on cyber impacts and policies.

3-ESTABLISH CYBER SECURITY PROFESSIONALS AS SRMA LIAISONS

With the challenging nature of the Health sector and the steady rise in cyber threats and incidents, there should be a cyber security professional within HHS to act as a strong, government liaison and advocate for the public private partnership when it comes to cyber matters. It has become increasingly apparent that industry needs a government representative who understands cyber security issues, threats, vulnerabilities and impacts as well as the blended threats between physical and cyber security. Having an established, clear government ‘go-to’ lead in this area is imperative to strengthening the partnership and improving the overall cyber security posture of the Health and Public Health sector.

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