Testimony of

Denise Anderson

On Behalf of the

The National Health Information Sharing & Analysis Center and the

National Council of Information Sharing and Analysis Centers

Before the

United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

April 4, 2017

ISAC BACKGROUND

Chairman Murphy and members of the Subcommittee, my name is Denise Anderson. I am President of the National Health Information Sharing & Analysis Center (NH-ISAC) and Chair of the National Council of ISACs (NCI). I want to thank you for this opportunity to address the Oversight and Investigations Subcommittee about the industry perspective on cybersecurity and information sharing as well as the importance of collaboration and coordination between the public and private 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 almost two decades.

ISACs are primarily 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 in order 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.

NCI BACKGROUND

The NCI is a voluntary organization of ISACs formed in 2003 in recognition of the need for the ISACs to share information with each other about common threats and issues. The mission of the NCI is to advance the physical and cyber security of critical infrastructure in North America by establishing and maintaining a framework for valuable interaction among and between the ISACs and with government. There are currently 21 individual ISACs that represent their respective critical infrastructure sectors or sub-sectors and 3 like organizations who are members of the NCI. The NCI has made it a goal to be inclusive of each critical infrastructure sector and sub-sector's operational arm.

The ISACs collaborate with each other daily through the NCI daily operations centers cyber call, and the NCI listserver. The NCI also hosts a weekly operations centers physical call and meets monthly to discuss issues and threats. The organization is a true cross-sector partnership engaged in sharing cyber and physical threats, mitigation strategies and working together and with government partners during incidents requiring cross-sector response as well as addressing issues affecting industry. In addition, the NCI conducts and participates in cross-sector exercises, works with the National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) during steady-state and incidents, holds emergency calls as needed and develops joint white papers around threats. The ISACs have been instrumental in embracing, developing and advancing the automatic exchange of data within their memberships and across the ISACs, as well as with government as possible.

ISACs AND GOVERNMENT PARTNERSHIPS

ISACs, which are not-for-profit organizations, work closely with various government agencies including their respective Sector Specific Agencies (SSAs) where they exist, intelligence agencies, law enforcement and state and local governments. In partnership with the Department of Homeland Security (DHS), several ISACs participate in the National Cybersecurity and Communications Integration Center (NCCIC) watch floor. ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the critical infrastructure sectors. Having ISACs on the floor has allowed for effective collaboration on threats and incidents and there have been many examples of successful information sharing. The ISACs also serve as liaisons to the National Infrastructure Coordinating Center (NICC) and play a vital role in incident response and collaboration under the Critical Infrastructure Partner Annex to the Incident Management Plan.

Finally, it should be noted that the ISACs collaborate with their sector coordinating councils as applicable and work with other critical infrastructure partners during steady state and incidents.

NH-ISAC BACKGROUND

The NH-ISAC, 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 200 organizations including healthcare delivery organizations (HDOs), pharmaceutical and medical device manufacturers, retail pharmacy, laboratory and radiological, electronic medical record providers and payers representing approximately one-third of the US Health and Public Health GDP*.

The NH-ISAC is a global organization that has members in several different countries and membership is growing rapidly.

Besides offering a trusted forum and community for sharing, the NH-ISAC offers a number of other services such as workshops, two annual summits, webinars, a daily report, monthly newsletter, white papers, special interest groups, a number of working groups and committees and various technical tools for member sharing. The ISAC provides alerts, has a representative on the NCCIC floor, and participates in exercises such as the national Cyberstorm series. The NH-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.

*Based on the annual revenue of all NH-ISAC member organizations. ($1.3 Trillion).

The NH-ISAC is also engaged in two ground-breaking initiatives. The first is the CyberFit suite of services that allows members to leverage the NH-ISAC community to realize cost savings and efficiencies.

Included in the initial suite of services is a third party risk assessment platform with over 80 questions tailored for healthcare organizations that will then be stored in an accessible database for the benefit of participating members, a benchmarking offering, as well as a 'shared security operations center (SOC)' program that will offer affordable services for malware analysis, penetration testing, vulnerability scanning and incident response.

The second is the Medical Device Security Information Sharing Council that is advancing efforts in the area of medical device security and safety. Under a Memorandum of Understanding between the NH-ISAC, the Medical Device Innovation, Safety and Security Consortium (MDISS), and the FDA; a number of national initiatives are underway to improve the security and safety of medical devices. These include: (1) MD-VIPER launched early this year to support the reporting of vulnerabilities and responsible medical device vulnerability disclosure per the FDA post market guidance (2) the National Cyber Safety Network for Health Technology, which leverages best public health practices to achieve national scale impact on patient safety and critical infrastructure and (3) the Medical Device Risk Assessment Platform, funded by DHS Cyber Security Division, a program for medical device assessments and threat intelligence with a database that HDOs use to understand and secure devices in their environment. Our programs include collaborations with DHS ICS-CERT, FDA, NIST National Cybersecurity Center of

Excellence, the Advanced Medical Technology Association (AdvaMed), manufacturers and national hospital networks as well as many other stakeholders.

NH-ISAC and MDISS also offer a community forum for manufacturers and HDOs to interact and collaborate through listservers, meetings, tracks at NH-ISAC summits, and workshops, among other things. The group has already held two medical device security workshops this year with many more scheduled and in February 2017, NH-ISAC and MDISS held an all-day medical device cybersecurity symposium at HIMSS, an industry conference.

The FDA has been very forward leaning in the medical device security collaboration space and the partnership with FDA, NH-ISAC and MDISS is a great example of how industry and government can come together to address cybersecurity issues. The partnership has been highly collaborative and is governed by a Memorandum of Understanding. Some examples of this public/private partnership include co-sponsoring of the FDA public workshop in January 2016, co-presenting at the FDA webinar on the post market guidance this past January 2017, presenting together at NH-ISAC Summits, and in particular, leveraging the NH-ISAC infrastructure for medical device vulnerability information sharing to meet the 'ISAO functionality' as described in FDA's post market guidance, as a regulatory incentive.

THE UNIQUE NATURE OF HEALTH AND CYBER

Six years ago, 'cyber' and 'healthcare' were not even placed in the same sentence. Today because of the proliferation of advances in technology and the efficiencies of connecting devices and data via the internet, 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 cannot deliver services, as was seen in several recent ransomware attacks, or data is manipulated or destroyed, patient lives can be at risk.

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. Coupled with a diverse base within the sector, 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 the CEO and Board level, and lack of cyber security strategy including a risk management approach, the health and public health sector faces an enormous challenge.

MEETING THE CHALLENGE

There are a number of great initiatives and efforts underway within the sector but there is still a lot more that can be done. Congress can help meet this challenge by focusing on four key areas:

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

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.

The SSAs 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 is an essential element of a successful cyber risk management strategy. Likewise, the most recent draft of the White House cybersecurity

executive order calls for an assessment of how government can support critical sectors' cyber risk management programs. Accordingly, one of our key recommendations in response to that review would be a policy statement that provides explicit guidance to SSA's and their sectors to integrate into their cyber risk management and preparedness programs their participation in and collaboration with these information sharing and incident response organizations where applicable.

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.

2-PROTECT INFORMATION SHARING

Recently, the Automotive ISAC was served a non-party deposition subpoena to furnish all documentation related to communications between the Auto ISAC and one of its members. The Auto ISAC with the help of other ISACs was able to quash the subpoena with Judge Wilkerson of the U.S. District Court for the Southern District of Illinois effectively ruling that the subpoena was nothing more than a fishing expedition.

The concern with this subpoena however, is that if Courts were to allow broad sweeps for information and using ISACs as "one-stop-shops" to accomplish it, such actions would effectively kill information sharing and undermine Congress' important information sharing goals set forth by the Cybersecurity Information Sharing Act (CISA) and the government's interest in promoting national security through the ISACs and public-private information sharing.

The confidential information shared amongst the members of an ISAC should be considered protected information and not subject to disclosure.

3-ELIMINATE THE CONFUSION BETWEEN THE TERMS ISAC AND ISAO

The Executive Order, Promoting Private Sector Cybersecurity Information Sharing, signed February 15, 2015 by President Obama is commendable in its intent to foster information sharing. Information Sharing and Analysis Organizations (ISAOs) were first defined in the Homeland Security Act of 2002. ISACs were created under Presidential Decision Directive 63 (PDD-63). Effectively ISACs were the original ISAOs and are the subject matter experts in information sharing with a majority of ISACs having been in existence for over a decade.

Indeed, there is a need for many groups that may not fall in with the critical infrastructure sectors such as legal and media and entertainment organizations, who are increasingly becoming targets for cyber incidents and attacks, to share information. The private sector is already organizing efforts in this area and as an example; the FS-ISAC, working with the legal industry, formed the Legal ISAO.

However, ISACs are much more than ISAOs. 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.

For example: enterprises can choose to obtain an intelligence feed to identify newly registered domains and choose to drop all email originating from newly registered domains. This is an example of a technique shared at last year's NH-ISAC Summit. This information is not shared in any other forum or event. Another example is the focus put on the adoption of the use of DMARC as a standard for improving trust in email and constraining the use of email for phishing attacks. This was initially shared at the FS-ISAC and today is offered through the NH-ISAC. These two examples have a material impact on improving industry resiliency and these techniques, like many others, are indicative of the unique services an ISAC offers to its members.

ISACs also serve a special role in critical infrastructure protection and resilience and play a unique role in the sector partnership model. While the White House has noted that the EO seeks to "not limit effective existing relationships that exist between the government and the private sector" the EO and prominent coverage of ISAOs has led to much confusion within industry as to the impacts to ISACs. It is absolutely essential that the successful efforts ISACs have established over the years should not be disrupted. It is clear that ISACs by their success meet the distinct and unique needs of each of their sectors and the owner and operator members of those sectors.

We have seen this clearly in the Health and Public Health Sector. When the FDA in its post market guidance for medical device security announced the need for manufacturers to participate in an ISAO, confusion ensued. The NH-ISAC is effectively serving as the ISAO and as mentioned is doing a large ground-breaking body of work in the medical device arena with the

FDA, but the guidance by using the term ISAO resulted in sector stakeholders immediately thinking some new organization needed to be created and has caused a lot of confusion that is still being sorted out.

The solution to easing this confusion is very simple. The White House, SSAs and other relevant agencies need to call out, recognize and support the unique role ISACs play in critical infrastructure protection and resilience and not apply the term ISAO as a blanket term for all information sharing. For instance, ISACs have the responsibility to maintain sector wide threat awareness within their respective sectors. It is critical that our federal partners continue to respect and support that role to avoid undermining one of the main duties of ISACs to their members and sectors. It is vital that the process is not diluted and remains streamlined to facilitate effective situational awareness and response activities particularly when an incident occurs.

4-ESTABLISH CYBER SECURITY PROFESSIONALS AS SSA LIAISONS

Given that cyber security has only recently come to healthcare, it is understandable that there has not been a need previously for a cyber security professional 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.

EFFECTIVE INFORMATION SHARING

It is important to note that the goal of information sharing is not to share information in and of itself but to create situational awareness in order to inform risk based decisions as well as 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.

The ISACs are successful organizations with almost two decades of proven case studies of information sharing and collaboration. They are the subject matter experts on information sharing. For information sharing to be effective it must be:

- Voluntary – not mandated or regulated
- Industry Driven
- Actionable, Timely and Relevant
- Bi-directional and Collaborative

Government can help this effort by:

- Encouraging owners and operators of critical infrastructure to join their respective sector ISACs
- Offering financial incentives such as tax breaks for owners and operators to join ISACs
- Recognizing ISACs and the unique operational role that they play in critical infrastructure protection and resilience

- Protecting information sharing by ensuring confidential data shared amongst members is protected from disclosure
- Place strong, defined and permanent cyber security liaisons and leadership within the SSAs to advocate the public private partnership when it comes to cyber matters. Cyber security liaisons and their leadership, should be experienced and certified cyber security professionals.

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