The Honorable Tim Murphy

1-I understand that HHS, apparently at the request of DHS, is establishing a Cybersecurity Communications and Integration Center specific to the health care sector, the "HCCIC." It would appear that this organization, at least on some level, replicates the role of an ISAC in other sectors.

1a-QUESTION: What is your understanding of this effort and how does it relate to your organization?

ANSWER: HHS recognizes the need to address the gaps in cybersecurity that are present within the Health and Public Health (HPH) sector. One way that HHS is seeking to address this gap is by standing up a center where all of the components of HHS; ONC, ASPR, FDA, for example, can come together to share and generate intelligence under one body and along with the private sector via the NH-ISAC in order to promote situational awareness and help mitigate against threats and incidents. HHS has reached out to NH-ISAC to take a collaborative partnership within the HCCIC in order to streamline information sharing broadly out to the HPH sector. The goal is to have NH-ISAC take a role in disseminating information from the HCCIC to the sector writ large through its established mechanisms.

1b-QUESTION: Based on your experience, are there other sectors that have their own CCIC?

ANSWER: In 2014, The US Department of the Treasury stood up the Cyber Intelligence Group (CIG) that essentially serves as the CCIC for the financial sector. The CIG's primary function is to distribute timely and actionable information and analysis that financial institutions can use to protect themselves. The CIG works very closely with the Financial Services Sector Coordinating Council (FSSCC) and the FS-ISAC. The collaboration and products delivered to the sector have been well received within the public/private partnership. The interaction demonstrated the importance of threat intelligence sharing and Treasury's role as a non-regulatory partner.

1c-QUESTION: Do you think this will be beneficial in addressing some of the challenges in the health care sector?

ANSWER: If the CIG model in Treasury is any indicator, the HCCIC should be successful if carried out as envisioned and if it is voluntary and non-regulatory in nature. This will result in improved dissemination within the sector. In addition, by bringing all of the components of HHS under one roof, increased situational awareness and cyber security efficiencies will result.

1d-QUESTION: Are there any potential downsides to having an HCCIC? If so what are they?

ANSWER: One potential downside of pulling together HHS components into one floor could be, a slow down of sharing from the private sector as 'government' is involved, Another downside could be that even though all of the components are brought together, sharing could still take place in a fragmented, unproductive manner. There could be risk of inadvertent disclosure or risk of post-hoc regulatory penalties for a reported breach. Finally if efforts are not effectively differentiated from the NCCIC environment, duplication of effort and additional costs for staffing and resources can result.

2-The public-private partnership model that we discussed at the hearing is designed so that the Sector Specific Agencies, Sector Coordinating Council, and Information Sharing and Analysis Centers work closely together to address sector challenges, in this case cybersecurity. QUESTION: How does the NH-ISAC work with HHS specifically as the health care SSA to address cybersecurity incidents and challenges?

ANSWER: NH-ISAC has worked with different components of HHS at various points and times. For example in the medical device security field, NH-ISAC along with the Medical Device Innovation and Safety Consortium (MDISS), has worked with FDA to establish workshops, carry out a medical device track at the NH-ISAC Annual Summit and to develop initiatives for responsible disclosure of vulnerabilities such as the MD-VIPER program. In addition, the ISAC is working with ONC and ASPR on the cooperative agreements to meet the deliverables as outlined in the Grant awards. The ISAC also coordinates on the NCCIC floor with HHS as applicable. NH-ISAC members are the first to work with MITRE and HHS to test out the ATT&CK model, a framework for describing the actions an adversary may take. The effort is currently underway.

2a-QUESTION: How does the NH-ISAC work with the SCC?

ANSWER: The NH-ISAC is a member of the Healthcare SCC and participates in monthly meetings, as well as some SCC working groups.

2b-QUESTION: Are there ways in which your organization could work more closely together with HHS and the Healthcare SCC?

ANSWER: There are always ways in which the ISAC can work together more closely with the SSA and the SCC. With the SSA, having that central coordinator role is so important to make sure there is less duplication of effort across the sectors and one point of contact to streamline communications and interactions. The SCC is primarily driven by volunteers at this point. The SCC requires a full-time dedicated resource(s) to drive the organization and the collaboration/mission of the private side of the HPH sector in order to be effective. The FS-ISAC funded such a full-time, Executive Director position at the FSSCC to serve the greater good of the sector. The NH-ISAC Board is currently exploring a similar type of funding/support situation.

3-My understanding is that there are multiple agencies within HHS that have pieces of healthcare cybersecurity. For example, the Office of Civil Rights deals with data breaches, the Food and Drug Administration deals with medical devices, and the list goes on for other components of the agency. QUESTION: How does the division of responsibilities affect the NH-ISAC?

ANSWER: With the preponderance of myriad components and roles within HHS, confusion, duplication of effort and a loss of threat landscape/situational awareness result. It is much easier to deal with one entity than several. The confusion is large. For example, when the HCCIC was announced questions immediately came from members regarding who they would report to. Would they report to the regulator, to the HCCIC, the NCCIC or other? Again, having one designated liaison/group to go to will be key to solving this problem.

3a-QUESTION: Would additional coordination or clarity by HHS regarding which pieces of the agency have responsibility for cybersecurity, and when, help your organizations.

ANSWER: Absolutely. It is very confusing and time consuming to try to figure out where to go to report and share information or seek coordination of efforts. During a time of crisis, time is of the essence so having one-stop sharing or at the very least a clear guideline as to where to go is essential.

3b-QUESTION: Do you have any suggestions for actions that HHS could take to better coordinate or clarify its cybersecurity roles and responsibilities.

ANSWER: The best step that HHS can take is to name a sector coordinator interfacing and speaking with one voice for HHS and with sufficient influence across the components, minimally at the assistant secretary level. Another step is to come up with a clear set of guidelines and definitions as to what the components are and what each role/responsibility is.

4-QUESTION: Do you believe a robust, centralized ISAC is important to elevating the security of the health care sector? In other words, why is a centralized ISAC more beneficial to the sector than perhaps a number of smaller entities organized around specific sub-sectors like the medical device ISAO?

ANSWER: Threats in general are typically seen across entire sectors. Differentiation amongst the sub-sectors usually lies in actors, actor motivation and then issues specific to the sub-sector.

Having a centralized ISAC provides may benefits; one place to go during incidents and daily sharing, entire sector perspective and sharing, one coordinating point with other sectors via the ISACs and with government, a true community that collaborates and coordinates together.
For example, one strength of the NH-ISAC is that we are able to bring all stakeholders together, providers and manufacturers, to address problems and threats together versus in silos. Indeed, as our industry expands and becomes increasingly internet connected and interconnected, threats seen in one subsector have rippling effects across other subsectors.

What the NH-ISAC has done is create special interest councils for the various sub-sectors such as medical devices, providers and pharmaceuticals. The benefit to this is that these members not only get access to all of the threat intelligence, best practice sharing and activity seen across the sector writ large, but also can share around threats and issues particular to their sub-sector community.

This has been done successfully in other ISACs such as the FS-ISAC where there are special interest groups for markets and exchanges, community banks and retail banks.

As a point of clarification, the medical device ‘ISAO’ is actually a special interest group within the NH-ISAC devoted to medical device security. The Council leverages the NH-ISAC infrastructure and member components. For example, the community includes health care delivery organizations (HDOs) as well as manufacturers and others across the sector who all have a stake in device security. The ISAC is able to build relationships and form partnerships so that all stakeholders can learn from each other and benefit by having one community instead of fragmented groups such as an HDO ISAO, a manufacturer ISAO or a pharmaceutical ISAO.

There is less duplication of effort and less costs and resources required by owners and operators to participate in one ISAC versus several ISAOs. The sector is very unique in that data must be portable across all components so components are actually dependent on each other. Therefore having one ISAC is the most efficient and cost-effective solution.

4a-QUESTION: What are the potential downsides or consequences of not having an effective ISAC for the entire sector?

ANSWER: The potential downsides include; fragmented sharing, loss of sector perspective and metrics, loss of a community of members helping members, confusion as to where to share information or to respond to for collaboration and communication, multiple and duplicative channels leading to ineffective coordination and threats becoming successful because not all are getting the information or are not receiving it in a timely fashion, ineffective coordination amongst other critical infrastructure and government agencies, extra resources and costs needed to share and coordinate amongst multiple channels. The more we can work together as one sector the more effective we can be and the more we can stay ahead of or on top of threats.

5.-My staff and I have heard from stakeholders in other industries, most notably the electricity sector, that they have broad, senior executive level engagement on their SCC, and that this engagement has significantly increased the effectiveness of the council and other aspects of their public-private partnerships, such as their ISAC. QUESTION: Who from your organizations participates in the Healthcare SCC?

ANSWER: If you look at the typical attendees of a healthcare SCC meeting, usually under 20 attendees, about 1/3 are comprised of private sector organizations such as NH-ISAC and HITRUST and 2/3 are comprised of GCC members and support staff. Very few owners and operators participate on the monthly calls.

5a-QUESTION: Would a similar model, with broad senior executive engagement on the SCC, work in the health care sector? Why or why not?

ANSWER: I do not believe that having HPH sector CEOs engage in the healthcare SCC would be productive. CEOs are not the subject matter experts when it comes to cybersecurity and have not traditionally been focused on cybersecurity. The better solution would be to appeal to CEOs and other C-Suite executives to dedicate cybersecurity experts who are aware of the full-range of cyber issues to participate in the SCC.

5b-QUESTION: Do you have any other thoughts on the SCC and its importance or the roles it plays in health care sector cybersecurity?

ANSWER: I think the SCC can play a very important role in assuring that cybersecurity policy is effective and aligned with the needs of the sector when it comes to its resilience and protection. As this sector is heavily dependent on other critical sectors like electricity, communications, and financial services, we need to work with those sectors to understand and manage interdependencies as they are affected by cyber threats, vulnerabilities and incident response. The SCC can offer a leadership perspective on the impacts of policy and regulation and can help play a coordination role for making sure industry's voice is heard on policy and regulatory issues that can affect the sector. For example, the FSSCC took an active role in helping secure clearances, developing fast-track incident response assistance by the government for financial services firms hit with overwhelming cyber attacks, and in securing access credentials during a physical incident such as Hurricane Sandy.

6-Based on the discussion from the hearing, it sounds like there is more that public-private partnerships could do to support smaller organizations. QUESTION: Do you have any suggestions for what HHS could do specifically to help smaller health care organizations better address cybersecurity?

ANSWER: There are many things HHS could do to help smaller health care organizations when it comes to cybersecurity. First, HHS could require in its audit components such as for HIPPA audits that during the audit process, a question is asked if the organization being audited is a member of the NH-ISAC as a best practice. Second, HHS could provide financial support or tax breaks or other incentives to smaller organizations that cannot afford cybersecurity tools such as DMARC or memberships in organizations such as the NH-ISAC. HHS could develop materials or courses that cover basic cyber hygiene or again can incent organizations to hire cyber security skilled staff. The SSA can push out guides that stress enterprise risk management and look at the consequences and impacts of not having a cyber security program in place. Much of this work has already been done through collaborative efforts of the public private partnership; namely, the NIST Cybersecurity Framework, which is a voluntary, consensus-based standard of practice that is seeing increasing uptake across the cyber risk management ecosystem.

6a-QUESTION: What about the Healthcare SCC?

ANSWER: The SCC could do many of the same things such as delivering a guide on basic cybersecurity hygiene and best practices as well as enterprise risk management and the impacts and consequences of not having a cyber security program in place. It could also develop papers on blended threats such as physical and cyber and what organizations can do to be aware of them.

7-QUESTION: Are there lessons from the progress of cybersecurity in the medical device sector that can benefit other parts of the health care sector, as well as the sector as a whole? If so, what are some of those lessons?

ANSWER: I think the major takeaway is that collaboration between all stakeholders, both public and private, is very important in order to create situational awareness and combat threats. We all need to work together to create an ‘army of good guys’. Over and over we tend to see that technology, while a contributor, is not really the problem. The problem is one of process and communication.

8-Your organization is the recent recipient of a grant from HHS for threat information sharing. Under that grant, the NH-ISAC is required to share threat information bi-directionally with the healthcare sector and HHS.

8a-QUESTION: Can you tell us more about that grant? Why is it important? What will it enable your organization to do?

ANSWER: There are two cooperative agreements, one issued by ONC and centered primarily on education and the other issued by ASPR and centered primarily on automated indicator sharing. The most important aspect for NH-ISAC when it comes to the agreements is that the ISAC was recognized as the channel for collaboration between HHS and the private sector. It takes any ‘noise’ off the table and clearly states that this is how the sector will work together and engage. It will enable us to be more effective and eliminates any distraction from the mission to educate and share. Again it is important to note that we are not inventing anything new to accomplish this. We are leveraging the already established information sharing channels that our members successfully engage in to mitigate against incidents.

8b-QUESTION: Have you seen an increase in NH-ISAC membership following the awarding of this grant?

ANSWER: While we’ve definitely seen interest in the ISAC perk up after the grants were awarded, we haven’t really seen a definitive up-tick in membership directly tied to the grant announcement at this point in time. The grant processes and milestones are still relatively new and we anticipate as goals are reached that over time we will be able to tie increased membership to some of the grant efforts.

8c-QUESTION: Has the awarding of this grant allowed you to increase your services? If so, how?

ANSWER: The grant processes and milestones are still relatively new and we anticipate as goals are reached that over time we will be able to tie increased services, such as basic cyber hygiene workshops and net flow traffic analysis and alerting to some of the grant efforts. It is important to note that many cyber security tools are costly and there is a limited dollar component to the grants. We fully expect to supplement the services we want to deliver as part of the grant from other NH-ISAC funding.

9-During the hearing, we talked a great deal about the HHS as the SSA, and the NH-ISAC, but we didn't really touch on the Government Coordinating Council. QUESTION: What role does the GCC play for each of your organizations?

ANSWER: Currently the role of the GCC is somewhat limited to the monthly meetings held between the GCC and the SCC. I think some of that is the result of the sector GCC and SSA components being very fragmented. Having HHS designate a sector liaison would go a long way to making the partnership more visible and effective.

9a-QUESTION: Are there additional initiatives that you believe that the GCC could take, or roles that it could fill, that would help your organizations and the health care sector as a whole better address cybersecurity.

ANSWER: I think as stated above, the more we can streamline and consolidate the interaction between the public and private sector collaboration, the better off all will be. If we can make the SCC and GCC more effective in what they do, collaboration and initiatives will be enhanced. There are also things like exercises that can be undertaken. A great example is the Hamilton series of exercises that were designed by the partnership and executed at the highest levels of Treasury, the financial GCC, the FSSCC and the FS-ISAC as well as eventually other sectors. Having the partnership in the HPH sector take the same steps would go a long way to identify and address gaps.

10-In your testimony, when discussing ISAOs, you state, "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."

10a-QUESTION: Can you elaborate on this point? How would the information sharing process be diluted and what are the potential consequences if this occurs?

ANSWER: Presidential Decision Directive 63 (PDD-63) states: "*...requires a **closely coordinated effort** of both the government and the private sector. To succeed, this **partnership must be genuine, mutual and cooperative**. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, we should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.*
*...**Close cooperation and coordination** is essential for a robust and flexible infrastructure protection program.*

*.... Information Sharing and Analysis Center (ISAC): The "government" shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of **a private sector information sharing and analysis center**. The actual design and functions of the center and its relation to the NIPC **will be determined by the private sector**...*"

The National Infrastructure Protection Plan calls for each sector to work together with its respective SSA, GCC, SCC and ISAC. During a time of crisis is is essential to have a streamlined process for sharing and a clearly designated body to collaborate and coordinate with.

Cyber threats and incidents happen instantaneously. When more than one body enters the mix, confusion ensues and efficiency and speed of information sharing and situational awareness is lost. Owners and Operators built the ISACs to serve as these conduits for information sharing and coordination. This model has existed for almost 20 years and it works. When owners and operators and the government do not know where to go or are forced to turn to several organizations, time and efficiency is wasted and attackers can get in. ISACs also offer a sector perspective. When other organizations chime in, the perspective is fragmented and the sector nuances are lost. For example, when the DDoS attacks of 2012/2013 occurred against the financial sector, the ISAC was able to report and provide analysis and information at a sector level versus having individual owners/operators or small groups report in. The information was coordinated and was instantaneous, relevant and actionable.

10b-QUESTION: Is that something that is happening in the health care sector or other sectors now?

ANSWER: Absolutely there is a lot of confusion in the HPH sector currently especially after FDA put out the Post-Market Guidance. The use of the term ISAO in the guidance has caused nothing but daily confusion and unnecessary effort. For some reason the expectation exists that a new ISAO needs to be stood up with all of the governance, legal, financial and other infrastructure required to effect information sharing. Instead the NH-ISAC is leveraging the power and the infrastructure that exists within the ISAC, which is essentially serving as the ISAO for medical devices. Manufacturers, stakeholders and government are getting ‘hung up’ on the term ISAO instead of using what already exists and running with it. It has stymied progress. Other sectors such as Finance are also encountering the confusion. There is a credit union ISAO, which is in conflict with the FS-ISAC.

10c-QUESTION: If so, how can we address it?

ANSWER: Government can address the issue by recognizing ISACs and the special operational role they play in critical infrastructure protection and resilience. Furthermore, government can help by encouraging owners and operators of critical infrastructure to join their respective sector ISACs and offer tax incentives or audit incentives to do so. Finally, government should stop using the term ISAO as a blanket term for all information sharing activities and instead refer to ISACs as ISACs and ISAOs as ISAOs.

This concludes my Answers to Additional Questions for the Record.