DATE: May 30, 2017

TO: House Energy & Commerce Committee,
Subcommittee on Oversight and Investigations

FROM: Terry Rice, VP, IT Risk Management & CISO,
Merck & Co., Inc.

SUBJECT: Answers to Follow-up Questions on Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships

2000 Galloping Hill Road
Kenilworth, NJ 07033 U.S.A.
T: 908-243-1929
E: terence_rice@merck.com

merck.com

Thank you for the opportunity to provide additional input on this important topic.

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.*

    a. *What is your understanding of the effort and how does it relate to our organization?* Representatives from HHS have discussed the notion of an HCCIC in conversation; however, I have not seen any written description of responsibilities and functions. Clearly, there is a need for better coordination among government healthcare entities at the federal, state, local, and tribal levels. This is an area in which the HCCIC could facilitate the flow of rapid and accurate information among all governmental healthcare entities. Information collected from state, local, and tribal entities could be correlated with federal data to present a more comprehensive picture of the threat facing the health care sector.

    The HCCIC could also serve as a bridge into the intelligence and law enforcement community on behalf of the sector. There is a strong argument given the diversity of the sector and the unique risks borne by each sub-sector component that an HCCIC could collect and process intelligence collection requirements against each of these risks. The HCCIC could aggregate information about sub-sector risks and convert those into a list of prioritized intelligence requirements/request for information against which the NCCIC/DHS, the US intelligence community and law enforcement might provide actionable information. This role would be akin to the way each of the military services maintains a small coordination presence within each of the major Department of Defense (DoD) intelligence agencies.

    The HCCIC could also serve as the primary coordination entity with governmental healthcare organizations around the world. While the provider and payer subcomponents of the US healthcare system are mostly based within the US, many

of the pharmaceutical, life sciences, medical device manufacturers, and health technology companies operate on a global scale and need information from non-US governmental entities to protect their overseas assets. This applies to both the physical as well as cyber threats.

The recent Wannacry ransomware incident is a great example of where international coordination among international healthcare entities could have helped to better protect multinational entities and arguably US domestic providers and payers. Apparently, lack of appropriate cyber intelligence sharing protocols and information dissemination policies hindered NHS from sharing actionable intelligence with its peers in HHS. The HCCIC could provide that bridge.

b. *Based on your experience, are there other sectors that have their own CCIC?* I am not aware of any of any other sector having its own CCIC; however, the Department of Treasury and the financial services industry created the Treasury Cyber Intelligence Group (CIG) to serve as the primary intelligence clearing house to/from the private sector. The CIG helps coordinate the collection and dissemination of timely intelligence from the federal government through the FS-ISAC and the Homeland Security Information Network (HSIN) as CIG Circulars. An example CIG Circular is attached.

   My understanding is the CIG also helps to coordinate the collection of information against prioritized intelligence requirements and requests for information coming from the private sector through the FS-ISAC. Cleared intelligence analysts within the CIG can identify the right sources and agencies from which to provide the information requested by the private sector.

c. *Do you think this will be beneficial in addressing some of the challenges in the health care sector?* Yes, it is likely be a positive development for the healthcare sector especially if the HCCIC were to operate the same roles and responsibilities as CIG.

d. *Are there any potential downsides to having an "HCCIC?" If so, what are they?* I see two potential downsides to the use of an HCCIC. The first is the possibility of creating additional confusion among the smallest members in the sector. These small companies already have local law enforcement, their local FBI office, DHS, and multiple Information Sharing and Analysis Organizations (ISAOs) claiming to be the primary gateway for their cyber intelligence requirements. This situation is made worse by the rapidly expanding network of private security intelligence firms. Smaller entities might be overwhelmed by another entity entering the mix especially if they have to manually correlate the data that comes from different intelligence sources. The larger healthcare companies have the personnel and/or tools to handle multiple data feeds from each of these entities simultaneously.

   The second issue is the possible duplication of effort between the HCCIC and the NCCIC. Given the well-reported shortage of cybersecurity professionals to meet the needs of government and industry, any redundancy would be a misuse of critical resources. This risk could be mitigated by having well-defined roles and responsibilities for the HCCIC that ensures that they do not duplicate the work of the NCCIC. This risk could be further mitigated by co-locating the HCCIC and NCCIC staff.

2. *According to the membership roster, each of your organization is a member of the Healthcare and Public Health Sector Coordinating Council. We know the Healthcare SCC has many roles and responsibilities beyond cybersecurity, but as cybersecurity becomes more important across the industry, the SCC will arguably have a big role to play. What services, products, or value does the SCC offer regarding cybersecurity?* The SCC currently conducts a monthly telecon for SCC members. Cybersecurity is a standing topic on the SCC agenda. At least one member of the SCC provides an update on cybersecurity matters; the update typically includes information on new threats, critical vulnerabilities, or emerging cybersecurity legislation and regulations. The SCC also conducts a joint session with the Government Coordinating Council (GCC) at least once a year. These tend to be 1-2 day events and are held in person in the Washington DC area. The joint sessions also include cybersecurity as a recurring topic.

    a. *Do you get the sense that their role and contributions are understood and appreciated across the sector?* No, there is limited participation by key members of healthcare sector in the SCC meetings. We need to have a much broader and more senior membership to make the SCC more effective.

    b. *Are there ways that the SCC could be more effective in assisting the sector with cybersecurity challenges?* As I stated in my previous testimony, one of the most significant ways that HHS could facilitate the growth and development of the SCC and the NH-ISAC is through the appointment and declaration of a private sector cybersecurity liaison whose primary purpose would be to educate senior executives within the sector on the benefits of participating in both of these organizations. The Financial Services SCC's and FS-ISAC's success was in part due to the strong and repeated endorsements by the Department of Treasury.

3. *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. Who from your organizations participates in the Healthcare SCC?* I am the primary participant in the SCC sessions.

    a. *Would a similar model, with broad senior executive engagement on the SCC, work in the health care sector? Why or why not?* Yes, as long as the agenda and topics of discussion were timely, relevant, and geared toward senior executive participation. There has been some inconsistency in the type and level of discussions within the Healthcare & Public Health (H&PH) SCC meetings most likely due to the broad backgrounds of those participating. The SCC should leverage more working groups and committees to increase participation at multiple levels.

    b. *Do you have any other thoughts on the SCC and its importance or the roles it plays in health care sector cybersecurity?* The SCC is still early in its maturity with respect to the topic of cybersecurity. There is a lot more that can be done in this area. For example, there is a group of approximately 75 CISOs from the healthcare industry that meet independently on a semiannual basis to discuss common topics of interest within the sector. The group often includes a representative from HHS. This group has twice volunteered to be the cybersecurity working group for the SCC.

The SCC should also consider the possibility of the NH-ISAC providing a full-time cybersecurity analyst to the SCC to handle and coordinate cybersecurity matters across the organization. This approach is like the one adopted by the financial services industry. This would provide a much-needed full time analyst to track the wide array of threats, vulnerabilities, regulations, and other rapidly changing variables that impact each SCC member's organization. The analyst would also handle any queries from the SCC members related to cybersecurity and route those to the NH-ISAC, the HCCIC, and/or the entity in the best position to the answer the request.

4. *As the Sector Specific Agency for the healthcare sector, HHS has a big role to play in guiding and supporting industry cybersecurity efforts. Can each of you briefly tell us how HHS, as the SSA for your sector, provides cybersecurity guidance and support for your organization?* HHS has several entities that provide some level of cybersecurity support and guidance for our organization. The Assistant Secretary for Preparedness and Response has the primary responsibility for healthcare and public health critical infrastructure protection. However, that organization's responsibilities go well beyond cybersecurity matters and cover any hazard that might disrupt or negatively impact the delivery. Consequently, there is limited depth in cybersecurity area. The HHS Chief Information Security Officer (CISO) is primarily responsible for protecting the assets, systems and information processed, stored, or transmitted within HHS. Traditionally, this role was focused internally. More recently the office has started working closely with the NH-ISAC and others to explore ways in which we can work together to secure the entire industry. The CISO's office has the greatest depth of cybersecurity skills and expertise.

   We also work with and receive guidance from the FDA's Center for Devices and Radiological Health. This organization has been the focal point for recent and emerging guidance concerning cybersecurity controls for medical devices and applications. Because the topic of cybersecurity often touches on the issue of privacy, we also work with the HHS Office of Civil Rights on privacy guidelines for the industry. Finally, given the rapidly expanding use of information technology within the healthcare industry, there are occasional interactions with the Office of the National Coordinator for Health IT.

   a. *Who in HHS, or what office, is considered the "go-to" contact for cybersecurity issues?* It is hard to pinpoint one office as the "go-to" contact today. The primary contact changes based on the specific topic and area in which a question or issue arises.

5. *My understanding is that 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. What parts of HHS does Merck work with when it comes to cybersecurity?* See previous response.

   a. *Does this division of cybersecurity roles and responsibilities at HHS complicate the ability of Merck to address cybersecurity within its products and organization?* While the division of responsibilities can make seeking cybersecurity guidance more complicated, this complexity has had limited impact on the security of our products and our organization. However, the lack of a central, cybersecurity liaison to the

private sector is likely to have more significant benefit to the smallest members of the healthcare system.

b. *Would additional coordination or clarity by HHS regarding which pieces of the agency have responsibility for cybersecurity, and when, help your organizations?* Yes, but the greatest beneficiaries are likely to be the smallest entities within the healthcare system

c. *Do you have any suggestions for actions that HHS could take to better coordinate or clarify its cybersecurity roles and responsibilities?* HHS should establish and appoint a senior level cybersecurity liaison to the private sector whose primary responsibility would be to educate senior business executives within the sector on the increasing cybersecurity risks that could impact critical healthcare operations. HHS should also consider conducting a series of "table top" exercises across the sector that challenge the cybersecurity policies, processes and procedures. These exercises can help to identify gaps and overlaps in responsibility as well as highlight areas that need additional focus by HHS and the sector. Last year's Cyberstorm V exercise, which was hosted by DHS, focused on retail and healthcare. This three-day exercise quickly identified a number of gaps. Unfortunately, DHS only conducts these exercises every two years and focuses on different industry sectors each time. HHS should take on responsibility for hosting healthcare specific exercises on a more frequent basis. The Hamilton Series hosted by the Department of Treasury is arguably the gold standard in this area.

   Another critical activity that HHS should pursue is the identification of the most critical assets across the sector whose loss or disruption could cause a national emergency. This analysis has been done at the highest level and only in the abstract terms. The assessment needs to be more detailed and clearly identify the most critical systems and dependencies. The output of this work should be used to select the scenarios for the exercises mentioned in the previous paragraph. However, the aggregation of this type of extremely sensitive information might cross into the classified realm and HHS needs to be able to support any requirements that stem from this (e.g. clearances for private sector members).

6. *The public-private partnership model depends on trust and collaboration between government and private sector participants. This can prove challenging in some sectors, such as health care, where the Sector Specific Agency (SSA) is also the regulator for that sector. Some sectors, such as financial services, have overcome these challenges to develop a robust relationship with their SSA. How much does the success of a public private partnership for cybersecurity depend on the level of trust and collaboration between private sector participants and their government counterparts, especially their sector specific agency?* Trust is the most critical enabler of any partnership, especially one in which parties agree to share sensitive information about their vulnerabilities and incidents. If a member feels that their information may be used for nefarious purposes or that others don't afford the information the same level of protection they would utilize in protecting this information internally, this will significantly inhibit information sharing. Trust is not something that can be regulated. Trust has to be developed and earned over time often with very small steps. One of the biggest challenges we had following the creation of the NH-ISAC was getting members to share data. Everyone was willing to receive data on Day 1. Very few were willing to share their own data. It took a couple of large companies which had previous

experience with information sharing in the defense and finance industries to commit to share before we started gaining traction. The broad and deep information that was shared between HHS and the ISAC during the recent Wannacry worm was a crucial step in further building that trust. The ISAC even sent an employee from one of the member companies to HHS Headquarters to participate in the incident response activities. That individual served as a bridge to and from the private sector. That individual also helped facilitate HHS access into a real-time chat service that was being utilized by threat analysts within the private sector. This went a long way to establish trust between the two entities.

a. *Is this a challenge in the health care sector, where HHS is the Sector Specific Agency but also serves as the regulator?* I don't think this is a specific problem within the healthcare sector. Many of the SSAs for other sectors also regulate the industries with whom they share intelligence. For example, the Department of Treasury (SSA for Finance) and the Department of Energy (SSA for Energy Sector).

   One issue that does create a unique disincentive within the health and public health sector is the publication of victims of breaches in which more than 500 health records have been exposed. This "wall of shame," as it is commonly referred to within the industry, does nothing to describe the state of security within the victim that was breached nor the sophistication of the attack used to gain access to the victim. Therefore, a well-defended organization that is breached by a nation-state actor suffers the same ignominy as a poorly defended organization that was breached by a novice hacker utilizing widely available tools.

   As I stated in my previous oral testimony, I believe that HHS should move toward a model more closely aligned with methods used by the National Transportation Safety Board investigates accidents and incidents with the goal of getting to the root cause and correcting any deficiencies especially those that might be systemic across the industry.

b. *Does the fact that different parts of the health care sector are regulated by different components of HHS complicate this relationship?* No, I don't think this is an issue. I think the model established by the Department of Treasury and its agencies (e.g. Office of the Comptroller of the Currency) have created an effective way to work together.

c. *Based on your experience, have other industries managed to navigate a similar situation, where their Sector Specific Agency is also their regulator? Or are there challenges unique to the health care sector its relationship to HHS that further complicate this dynamic?* Yes, I believe the Financial Services Industry, the Energy Sector, and the Defense Industrial Base have established trust and processes to facilitate and encourage the sharing of threat, vulnerability, and incident data.

7. *Your organization is obviously larger and more well-resourced than a rural hospital or small physician practice. We've seen in other cases like the Target breach, however, that smaller organizations can be the " infection points" for larger organizations, due to the way that business relationships and networks are set up. Recognizing that cybersecurity is a collective responsibility, how do - or can - larger organizations assist in bolstering awareness and engagement of smaller participants in the sector?* There is a tremendous potential for larger and better resourced organizations to share the policies, procedures, techniques, and

solutions with smaller entities across the sector. To this end, the NH-ISAC has created a number of working groups that are seeking to leverage the resources of the larger members but with input from all to develop capabilities that can be shared across the sector. For example, the NH-ISAC Big Data and Analytics Working Group published a guide on the security of big data services that can be utilized by all members of the ISAC. The NH-ISAC Threat Intelligence Working Group has tasked a number of the largest members to write software code to help identify specific types of attacks within organization. This code will be donated freely to other healthcare members. Finally, approximately ten of the largest healthcare companies within the NH-ISAC have funded an effort called Cyberfit to create a suite of shared services that would have standardized terms and conditions of use and aggressive, pre-negotiated pricing. Initially these services would function as a group purchasing arrangement in which one or more vendors would provide the Cyberfit services but over time the NH-ISAC consider making these internal services provided by the NH-ISAC.

a. *Are there factors that impede collaboration within the sector?* There are two issues that have been discussed as impeding collaboration with the sector. The first is the Stark Law which is designed to prohibit physician self-referral. Some entities, particularly providers, have raised concern that the use of shared cybersecurity services could be interpreted as a violation of the Stark Law. One way this issue could be addressed is to create a specific exemption for cybersecurity services.

   The second topic of concern is the potential for eDiscovery requests to impede sharing within an ISAC. If organization A suffered a breach and entered into litigation, there is the possibility that opposing council could serve the ISAC with a discovery request to show that organization A was less protected than other members of the ISAC or opposing council could use the same discovery request to find other victims of the same attack and potentially widen the case. We recently noted that the Auto-ISAC received a discovery request as a result of litigation one of its members was facing. Fortunately, the discovery request was quashed but the issue had a chilling effect on information sharing by a number of members within the healthcare industry.

8. *During the hearing, we talked a great deal about the HHS as the SSA, and the NH-ISAC, but didn't really touch on the Government Coordinating Council. What role does the GCC play for your organization?* The GCC plays a very limited role. In fact, the only interaction we have is during the semi-annual meetings that are conducted between the GCC and SCC. There is lots of room to improve this dialogue. In fact, I believe that both the GCC and SCC should have cyber working groups that would work closely together throughout the years on cybersecurity topics that are relevant to the industry. If the such a mechanism were in place, the need for a Healthcare Industry Cybersecurity Task Force might have been obviated.

   a. *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?* The most immediate activity would be to take a co-sponsorship role in conducting a series of cybersecurity "table top" exercises with the SCC, the HCCIC, and the NH-ISAC. It is very likely these exercises would highlight a large number of other possibilities for improvement. The Defense and Finance industries have found similar exercises invaluable.

9. *Would you support HHS making a recommendation that encourages participation in the ISAC?* Absolutely and unequivocally yes.

    a. *Do you believe that it would improve the functioning of the ISAC, and therefore cybersecurity across the sector, for HHS to make such a recommendation?* Yes, particularly if that recommendation were directed to the senior executives (e.g. CEO and executive committees) at each entity within the healthcare industry. Most of the cybersecurity professionals already understand the benefits of information sharing. Getting senior executive sponsorship is likely to remove any real or perceived obstacles to sharing.

    b. *Do you think there are potential consequences- real or perceived - from HHS taking this approach?* No.

10. *Recently in the cybersecurity community, there has been some confusion regarding ISACs and ISAOs. Do you think that this confusion has caused any issues with regards to cybersecurity protocol- specifically facilitating effective situational awareness and response activities, particularly when an incident occurs?* Yes. I think there has been a tremendous amount of confusion in the use of the term ISAO and ISAC. I have rarely heard two or more individuals offer consistent definitions of these terms. Part of the confusion stems from the fact many of the sixteen critical infrastructure sectors had not established an effective or well-recognized ISAC when the concept of an ISAO was introduced through Executive Oder 13691. Following publication of the EO, a wide array of existing associations, organizations, and companies attempted to brand themselves as ISAOs. While these additional groups may be helpful for sub-sector components or within geographic areas, it has made it hard for the NH-ISAC to recruit members.

    a. *What do you think should be done to address this confusion?* I think each sector specific agency should identify who the ISAC is for their respective sectors so there is no confusion. Additional information sharing mechanism should be encourage but there should be no dispute on which entity is the primary ISAC for each critical infrastructure sector. For the healthcare sector, HHS should clearly specify that the NH-ISAC is the ISAC for the health and public health sector but that it also encourages members of the sector to also participate in other ISAOs that help meet their business needs

<u>The Honorable Buddy Carter</u>

1. *When we think about cybersecurity and health, most people seem to understand the dangers regarding privacy of their personal health information. But, what most people don't know is that this kind of theft can have a direct impact on your health. As a pharmacist, I also know that if we don't catch medical identity fraud, it can have serious physical consequences for patients. Can you elaborate on the consequences of medical identity theft?* Cybersecurity professionals generally think about three consequences that stem from any security incident. First is the <u>loss of confidentiality</u> of sensitive information. Second, is the <u>loss of integrity</u> of critical data. The third is the <u>loss of availability</u> of data, service or function. In the case of medical identity theft, all three consequences can occur often each with the potential to cause significant patient harm. When confidential personal health information is exposed, the data can be used to conduct fraud. In fact, recent incident data

indicates there has been an uptick in Health Savings Account/Flexible Spending Account theft given the large amount of medical information that has been exposed over the past couple of years. Confidential healthcare information can also be used to extort money from, or blackmail victims, particularly if their compromised healthcare information includes medical issues that have a social stigma. Medical identity theft can also lead to data integrity issues in health records if the stolen information is used to receive medical services. In this situation, accurate information in the victim's medical file may be overwritten by data from the person impersonating the victim which could lead to harm the next time the victim receives medical treatment. Finally, a thief may use stolen credentials (e.g passwords) to gain access to the patient's records and delete data or modify data that could make the information inaccessible to the victim and/or medical professionals. This loss of availability could cause patient harm.

2. *The GAO recently released a study analyzing Identify Theft Services. The report details the dangers that we have discussed here. Have you reviewed the study? How do you propose we counter these very real threats to our health care?* Yes, I am aware of and have reviewed the study. I believe there are at least two initiatives that could reduce the likelihood of medical identity theft. The first is to prohibit the use of the Social Security Number as a primary authenticator to any health system or service. Given the wide array of personal information breaches that have occurred over the last 5-10 years, SSNs are frequently available for sale on illicit online services. A criminal can often gain the SSN of a victim he/she wants to target by utilizing one of these illicit services. Therefore, SSNs should never be used as a mechanism for verifying a user's identity.

   The second recommendation is to use strong identity and access mechanisms to gain access to health information and services. The National Institute for Standards and Technology (NIST) and the office responsible for the National Strategy for Trusted Identity in Cyberspace (NSTIC) have developed standards that can be used to gain higher levels of assurance than a simple username and password. These standards are increasingly used throughout government and industry to protect the most sensitive transactions and information. In fact, following the OPM breach many government offices mandated the use of these standards for all federal employees. Within the healthcare and pharmaceutical industry, the SAFE Biopharma Association has adopted the same standards, with a few industry specific amendments, and they are used to protect clinical trials, sign drug prescriptions, and provide authentication into sensitive cloud services. Healthcare regulators in the US, EU, and Japan now accept the SAFE Biopharma standard as an authorized means of identity verification and validation in new drug application submissions. While there is still work that would need to be done to improve ease of use these standards offer a promising way to significantly reduce medical identity theft.