GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

April 27, 2017

Ms. Denise Anderson
President
National Health Information Sharing and Analysis Center
226 North Nova Road
Suite 391
Ormond Beach, FL 32174

Dear Ms. Anderson:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, April 4, 2017, to testify at the hearing entitled "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Thursday, May 11, 2017. Your responses should be mailed to Elena Brennan, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Elena.Brennan@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Attachment—Additional Questions for the Record

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 this effort and how does it relate to your organization?

    b. Based on your experience, are there other sectors that have their own CCIC?

    c. Do you think this will be beneficial in addressing some of the challenges in the health care sector?

    d. Are there any potential downsides to having an "HCCIC?" If so, what are they?

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. How does the NH-ISAC work with HHS specifically, as the health care SSA, to address cybersecurity incidents and challenges?

    a. How does the NH-ISAC work with the SCC?

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

3. 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. How does the division of responsibilities affect the NH-ISAC?

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

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

4. 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?

    a. What are the potential downsides or consequences of not having an effective ISAC for the entire sector?

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. Who from your organizations participates in the Healthcare SCC?

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

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

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

    a. What about the Healthcare SCC?

7. 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 these lessons?

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.

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

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

    c. Has the awarding of this grant allowed you to increase your services? If so, how?

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. What role does the GCC play for each of your organizations?

    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?

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."

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

b. Is that something that is happening in the health care sector – or other sectors – now?

c. If so, how can we address it?