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

MEMORANDUM

April 1, 2017

To: Subcommittee on Oversight and Investigations Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Hearing on "Cybersecurity in the Heath Care Sector: Strengthening Public-Private Partnerships"

On **Tuesday, April 4, 2017, at 10:15 a.m. in room 2322 of the Rayburn House Office Building**, the Subcommittee on Oversight and Investigations will hold a hearing titled "Cybersecurity in the Heath Care Sector: Strengthening Public-Private Partnerships."

I. INFORMATION SHARING PROTECTS CRITICAL INFRASTRUCTURE

The United States has long sought to address security risks to the nation's critical infrastructure, which includes essential physical or cyber assets that support economic and governmental operations.[1] The majority of critical infrastructure resources are

[1] Government Accountability Office, *Critical Infrastructure Protection: DHS Has Made Progress in Enhancing Critical Infrastructure Assessments, but Additional Improvements are Needed* (Jul. 2016) (GAO-16-791T).

owned and operated by the private sector.[2] The nation's health care system is an example of critical infrastructure.[3]

II. CYBERATTACKS CONTINUE TO IMPACT THE HEALTH CARE SECTOR

Cyberattacks are a growing threat to the health care sector. More than 113 million medical records were reportedly compromised in 2015.[4] Recent cyberattacks have attempted to disrupt hospital operations through the seizure and ransom of personal health records.[5] In addition, reports have indicated that medical devices such as pacemakers, insulin pumps, and defibrillators are also vulnerable to cyberattacks.[6]

Health insurance computer systems have also experienced breaches recently, further underscoring the need for effective health care cybersecurity. For example, in 2015, a cyber security breach at Anthem, a health insurance company, compromised the personal information of 78.8 million consumers.[7] The breach was one of the largest hacks ever of insurance company customer data, and a California Department of Insurance investigation concluded, with a significant degree of confidence that the attacker was acting on behalf of a foreign government.[8]

III. STRENGTHENING HEALTH CARE SECTOR CYBERSECURITY THROUGH INFORMATION SHARING

Information sharing is crucial to protecting critical infrastructure. To that end, federal policy has encouraged the voluntary creation of information sharing and analysis

---

[2] Government Accountability Office, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely* (Feb. 2017) (GAO-17-163).

[3] The White House, *Presidential Policy Directive - Critical Infrastructure Security and Resilience* (www.obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/) (accessed Mar. 28, 2017).

[4] *Has Health Care Hacking Become an Epidemic*, PBS News Hour (Mar. 23, 2016).

[5] *Los Angeles Hospital Pays Hackers $17,000 After Attack*, The New York Times (Feb. 18, 2017).

[6] *Medical Devices are the Next Security Nightmare*, Wired (Mar. 3, 2017).

[7] California Department of Insurance, *Investigation of Major Anthem Cyber Breach Reveals Foreign Nation Behind Breach* (Jan. 6, 2017) (press release).

[8] *Id.*

centers (ISACs) to meet the information-sharing needs of different industry sectors.[9] ISACs are comprised of private-sector owners and operators of critical infrastructure, and are designed to facilitate information sharing and protection among members. Federal agencies also collaborate with ISACs to facilitate the sharing of cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.[10]

The National Health Information Sharing and Analysis Center (NH-ISAC) is the ISAC for the nation's health care and public health sector.[11] Members of the NH-ISAC include providers, health information technology companies, insurers, medical device manufacturers, and laboratory, blood, and pharmaceutical organizations.[12] To help members protect against cyber and physical security threats, the NH-ISAC states that it disseminates threat information to members and helps them enhance the resiliency of their cybersecurity systems.[13]

IV. WITNESSES

The following witnesses have been invited to testify:

Denise Anderson
President
National Health Information Sharing and Analysis Center

Michael McNeil
Global Product Security and Services Officer
Philips Healthcare

Terry Rice
Vice President, IT Risk Management and Chief Information Security Officer
Merck & Co., Inc.

---

[9] Government Accountability Office, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors* (Jul. 2004) (GAO-04-780).

[10] See note 2.

[11] National Health ISAC, About National Health Information Sharing and Analysis Center (www.nhisac.org/about-nhisac/) (accessed Mar. 23, 2017).

[12] National Council of ISACs, Member ISACs (www.nationalisacs.org/member-isacs/) (accessed Mar. 23, 2017).

[13] *Id.*