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

June 5, 2017

To: **Subcommittee on Oversight and Investigations Democratic Members and Staff**

Fr: **Committee on Energy and Commerce Democratic Staff**

Re: **Hearing on "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity"**

On **Thursday, June 8, 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 "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity." This hearing will focus on the role of the Department of Health & Human Services (HHS) in protecting the health care sector from cyberattacks.

I. THE FEDERAL GOVERNMENT AND THE HEALTH CARE SECTOR ARE VULNERABLE TO CYBER ATTACKS

Cybersecurity has long been a challenge for the health care sector, including both HHS and private sector systems. Recent cyberattacks have disrupted hospital operations through the seizure and ransom of personal health records.[1] In addition, reports indicate that medical devices, such as pacemakers, insulin pumps, and defibrillators are also vulnerable to cyberattacks.[2] According to HHS, more than 16 million medical records were compromised in 2016, and more health care entities were victims of cyberattacks in

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

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

2016 than in any year since HHS began publishing such data in 2009.[3] Health insurance computer systems have also experienced breaches. For example, in 2015, a cybersecurity breach at Anthem Inc. compromised the personal information of 78.8 million consumers.[4]

Ransomware attacks are a common type of cyberattack confronting the health care sector. Ransomware is a form of malware that encrypts a victim's digital files and then demands a payment to unlock the files.[5] The recent WannaCry ransomware attack, for example, crippled 200,000 computers in more than 150 countries.[6] WannaCry had a particularly damaging effect on health care services in the United Kingdom, where doctors in affected hospitals were unable to access patient files, and emergency rooms had to turn away urgent care patients.[7]

A new report released on June 2, 2017 from the Health Care Industry Cybersecurity Task Force – a public-private partnership established by the *Cybersecurity Act of 2015* – found that "health care cybersecurity is a key public health concern that needs immediate and aggressive attention."[8] The report identified key areas to increase cybersecurity within the health care sector, including: identifying measures to protect research and development, better information sharing of industry threats and risks, and streamlining governance for health care cybersecurity.[9] Emery Csulak, a Co-Chair of the Health Care Industry Cybersecurity Task Force, is appearing as a witness for this hearing.

II. FEDERAL AND PRIVATE SECTOR EFFORTS TO BOLSTER HEALTH CARE CYBERSECURITY

[3] *Largest Healthcare Data Breaches of 2016,* HIPAA Journal (Jan. 4, 2017); 42 U.S.C. § 17932(e)(3); 42 U.S.C. § 17932(e)(3) (requiring entities that handle unsecured protected health information to report breaches to HHS, and for HHS to post on its website breaches affecting more than 500 people).

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

[5] The Federal Bureau of Investigation, *Incidents of Ransomware on the Rise* (Apr. 29, 2016) (www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise).

[6] *What We Know and Don't Know About the International Cyberattack*, New York Times (May 12, 2017).

[7] *Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool,* New York Times (May 12, 2017).

[8] Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Health Care Industry* (June 2, 2017) (https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf).

[9] *Id.*

The Department of Homeland Security (DHS) developed the National Cybersecurity and Communications Integration Center (NCCIC) as the central place for federal and private sector organizations to address cyber-related threats and respond to cyberattacks.[10] DHS NCCIC also coordinates cyber-related activities, such as the dissemination of indicators to federal departments and agencies.[11]

In discussions with committee staff, HHS officials stated that they plan to assist both HHS component agencies and private health sector companies in responding to cyberattacks. Agency officials stated that HHS's aim is to collaborate with DHS NCCIC to collect cyber information and share it with HHS agencies and the private health care sector.[12]

The private sector owns and operates the majority of critical infrastructure resources.[13] Information sharing is crucial to protecting this critical infrastructure, and federal policy has encouraged the voluntary creation of information sharing and analysis centers (ISACs) in different industry sectors comprised of private-sector owners and operators of critical infrastructure.[14] Federal agencies collaborate with ISACs to facilitate the sharing of cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.[15]

The National Health Information Sharing and Analysis Center (NH-ISAC) is the ISAC for the nation's health care and public health sector.[16] Members of the NH-ISAC include providers, health information technology companies, insurers, medical device manufacturers, and laboratory, blood, and pharmaceutical organizations.[17] To help members protect against cyber and physical security threats, the NH-ISAC disseminates threat information to members and helps them enhance the resiliency of their

[10] U.S. 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).

[11] *Id.*

[12] Briefing by HHS officials to House Committee on Energy and Commerce Staff (May 10, 2017).

[13] *See* note 10.

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

[15] *See* note 10.

[16] NH-ISAC, About National Health Information Sharing and Analysis Center (www.nhisac.org/about-nhisac/) (2017).

[17] National Council of ISACs, Member ISACs (www.nationalisacs.org/member-isacs/) (2016).

cybersecurity systems.[18] The NH-ISAC faces a number of organizational and operational challenges. The subcommittee addressed this topic in an April 4, 2017 hearing, which was titled, “Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships.”

III. WITNESSES

The following witnesses have been invited to testify:

Steve Curren
Director for the Division of Resilience
Office of Emergency Management
Office of the Assistant Secretary for Preparedness and Response
U.S. Department of Health & Human Services

Leo Scanlon
Deputy Chief Information Security Officer
U.S. Department of Health & Human Services

Emery Csulak
Chief Information Security Officer and Senior Privacy Official
Centers for Medicare & Medicaid Services
Co-Chair, Health Care Industry Cybersecurity Task Force

[18] *Id.*