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 9, 2017

To: **Subcommittee on Communications and Technology Democratic Members and Staff**

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

Re: **Hearing on "Cybersecurity Risks to Wireless Networks"**

On **<u>Tuesday, June 13, 2017, at 10:00 a.m. in room 2322 of the Rayburn House Office Building</u>**, the Subcommittee on Communications and Technology will hold a hearing titled "Promoting Security in Wireless Technology."

I. BACKGROUND

Wireless technology has become ubiquitous in the lives of many Americans. According to some reports, the use of mobile networks has increased 18-fold over the past five years.[1] Wireless networks connect to wired networks and consumer devices of all kinds across the globe. The centrality and interconnected nature of these networks is highlighted by recent cyberattacks that jump from network to network and from device to device.

One such attack relates to recent demonstrations of how some wireless networks are vulnerable to a security flaw in Signaling System Seven.[2] This vulnerability was later used to intercept two-factor authentication codes to drain unsuspecting customers' bank accounts.[3] Last year, the Mirai Botnet—comprised in part of wirelessly connected video cameras—unleashed a

[1] Cisco, *Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper* (Feb. 2017) (www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html).

[2] *After Years of Warnings, Mobile Network Hackers Exploit SS7 Flaws to Drain Bank Accounts*, The Register (May 3, 2017) (online at www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/).

[3] *Id.*

denial of service attack that brought down some of the most frequented sites on the internet. Cybercriminals have recently even targeted 9-1-1 call centers by taking control of consumers' mobile phones to have them repeatedly dial 9-1-1, effectively blocking legitimate 9-1-1 calls.[4]

Just a few weeks ago, hackers used software called "WannaCry" to attack networks worldwide, demanding that users pay or risk having their data deleted. The malware spread to over 150 countries in over two days, impacting more than 10,000 organizations, including shutting down work at 16 United Kingdom hospitals.

II. FEDERAL ROLE IN CYBERSECURITY

Over the years, the federal government has taken some steps to help increase the security of the nation's networks.

- **National Coordinating Center for Communications (NCC):** The NCC monitors cybersecurity events that affect the nation's emergency communications networks with the aid of the U.S. Computer Emergency Response Team. The NCC also serves as the cyber information sharing and analysis center for the telecommunications industry.
- **Protected Critical Infrastructure Information Program:** Under the Critical Infrastructure Information Act of 2002, critical infrastructure companies may disclose cyber threats and vulnerabilities to the government in exchange for some protection from liability stemming from those disclosures.
- **Federal Communications Commission (FCC):** The FCC has traditionally taken an active role in cybersecurity. The FCC has adopted consumer data security protections, launched an inquiry on cybersecurity for 5G networks, and published a whitepaper outlining gaps in the nation's cybersecurity policy generally. The current administration has signaled in recent months, however, that it will step back from these responsibilities.
- **Department of Commerce (Commerce):** The National Telecommunications and Information Administration (NTIA), within Commerce, has convened several multistakeholder meetings aimed at improving cybersecurity and vulnerability disclosure. The National Institute for Standards and Technology (NIST), also within Commerce, produces a voluntary framework for critical infrastructure organizations to better manage cybersecurity risks. NTIA released a request for comment on June 8, seeking input from stakeholders on actions to take to mitigate threats from botnet attacks and the role of government. Commerce and NIST also will host a public workshop in July entitled "Enhancing Resilience of the Communications Ecosystem."

III. DEMOCRATIC LEGISLATIVE PROPOSALS

Democratic members of the Communications and Technology Subcommittee introduced three bills to address cybersecurity risks earlier this Congress:

[4] *Teen Arrested After Forcing Phones to Call 911 Nonstop*, Gizmodo (Oct. 28, 2016) (online at gizmodo.com/teen-arrested-after-forcing-phones-to-call-911-nonstop-1788329521).

- H.R. 1335, the Cybersecurity Responsibility Act, introduced by Rep. Clarke (D-NY), would require the FCC to adopt cybersecurity rules protecting domestic communications networks from cyberattacks.

- H.R. 1340, the Interagency Cybersecurity Cooperation Act, introduced by Rep. Engel (D-NY), requires the FCC to create an interagency committee whose mission is collecting and reviewing information on cybersecurity incidents. The committee should then use its findings to recommend investigations and issue reports to Congress outlining relevant findings and policy recommendations.

- H.R. 1324, the Securing IoT Act, introduced by Rep. McNerney (D-CA), requires Internet of Things (IoT) devices, and other wireless devices, to be certified as complying with cybersecurity standards.

IV. WITNESSES

The following witnesses have been invited to testify:

Bill Wright
Director
Government Affairs & Senior Policy Counsel, Symantec

Amit Yoran
Chairman and CEO
Tenable Network Security

Dr. Charles Clancy
Director and Professor
Hume Center for National Security and Technology, Virginia Tech
On behalf of CTIA—The Wireless Association

Kiersten E. Todt
Former Executive Director, Commission on Enhancing National Cybersecurity; Managing Partner, Liberty Group Ventures, LLC; Resident Scholar, University of Pittsburgh Institute for Cyber Law, Policy, and Security