FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH 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

November 14, 2016

To: Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Hearing on "Understanding the Role of Connected Devices in Recent Cyber Attacks"

On Wednesday, November 16, 2016, at 10:00 a.m. in room 2175 of the Rayburn House Office Building, the Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology will hold a joint hearing titled "Understanding the Role of Connected Devices in Recent Cyber Attacks."

I. BACKGROUND

An unknown group attacked a key part of the internet's infrastructure on October 21, 2016.[1] These attackers targeted a domain name service (DNS) provider called Dyn. Domain name service providers such as Dyn give popular websites access to the basic technical capabilities necessary to reach large numbers of consumers.[2] The attack began at 7 a.m. and occurred in three waves, spreading westward across the United States throughout the day.[3] By attacking Dyn, the hackers took down some of the most frequented sites on the internet, including Twitter, Amazon, Spotify, and Airbnb for large portions of the day.[4]

---

[1] *What We Know About Friday's Massive East Coast Internet Outage*, Wired (Oct. 21, 2016) (www.wired.com/2016/10/internet-outage-ddos-dns-dyn/).

[2] *See id.*

[3] *Internet of Things' Hacking Attack Led to Widespread Outage of Popular Website*, NPR (Oct. 22, 2016) (www.npr.org/2016/10/22/498954197/internet-outage-update-internet-of-things-hacking-attack-led-to-outage-of-popula).

[4] *See id.*

The Dyn attack was a "distributed denial of service," or DDoS, attack.[5] A DDoS attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.[6] Coordinated attacks such as the Dyn attack are often perpetrated by "botnets."[7] A botnet is a network of private computers or devices infected with malicious programming, controlled as a group, without the owners' knowledge.[8] By employing a botnet, a single nefarious actor can take over millions of computers and devices at a time and focus all of the infected machines on a single entity.[9]

The group responsible for the Dyn attack used a botnet called "Mirai."[10] The Mirai botnet is unusual in that it is not made up of standard computers.[11] Rather it comprises connected devices such as webcams and digital video recorders.[12] The program that created the Mirai botnet scans the internet for poorly secured devices every few minutes.[13] This particular botnet was able to infect 400,000 devices using a list of only 60 default usernames and passwords.[14] Many of these weak default passwords were hard-wired into the devices so they could not be changed by their owners.[15]

Connected devices like those hijacked in the Dyn attack are sometimes called Internet of Things (IoT) devices. These devices make up an ever-growing percentage of the machines connected to the internet. A recent report predicted that between 2015 and 2020, the number of

---

[5] *What We Know About Friday's Massive East Coast Internet Outage*, Wired (Oct. 21, 2016) (www.wired.com/2016/10/internet-outage-ddos-dns-dyn/).

[6] *Hacker Lexicon: What Are DoS and DDoS Attacks?*, Wired (Jan. 1, 2016) (www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/).

[7] *See id*.

[8] *Botnet Malware: What It Is and How to Fight It*, WeLiveSecurity (Oct. 22, 2014) (www.welivesecurity.com/2014/10/22/botnet-malware-fight/).

[9] *Hacker Lexicon: What Are DoS and DDoS Attacks?*, Wired (Jan. 1, 2016) (www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/).

[10] *How One Rent-a-Botnet Army of Cameras, DVRs Caused Internet Chaos*, Ars Technica (Oct. 25, 2016) (arstechnica.com/information-technology/2016/10/inside-the-machine-uprising-how-cameras-dvrs-took-down-parts-of-the-internet/).

[11] *See id*.

[12] *See id*.

[13] *IoT Botnet Highlights the Dangers of Default Passwords*, Computer World (Oct. 3, 2016) (www.pcworld.idg.com.au/article/607908/iot-botnet-highlights-dangers-default-passwords/).

[14] *Id.*

[15] *See id*.

IoT connections will grow nearly 2.5-fold, from 4.9 billion in 2015 to 12.2 billion in 2020.[16] By 2020, IoT devices will account for nearly half of all machines connected to the internet.[17]

II. THE ROLE OF DEVICE MANUFACTURERS AND INTERNET SERVICE PROVIDERS

Many IoT devices are particularly vulnerable to cyberattacks. IoT device manufacturers are often slow to patch vulnerabilities and many devices do not have the capacity to run anti-malware solutions. To address the security flaws that bolstered the ranks of the Mirai botnet, several IoT device manufacturers have started requiring users to create unique passwords for their devices.[18] Some have even issued recalls for their insecure IoT devices.[19]

In the wake of the Dyn attack, some have argued that Internet Service Providers (ISPs) might be uniquely situated to combat botnets. The Federal Communications Commission's (FCC) 2015 Open Internet Order does generally prohibit ISPs from blocking non-harmful devices from accessing the network.[20] The FCC rules contain a specific exemption that permits ISPs to take action to fend of DDoS attacks on specific network infrastructure elements.[21] The Computer Fraud and Abuse Act, however, may prohibit service providers, and other entities, from taking defensive measures related to an attack.[22]

To the extent that ISPs wish to share data related to a cyber threat, ISPs are authorized to do so under the Cybersecurity Information Sharing Act of 2015 (CISA).[23] CISA allows an ISP, as a non-federal entity, to monitor its system and share cyber threat indicators with others for a cybersecurity purpose.[24] As it relates to sharing information, CISA preempts all other federal or

---

[16] *IoT Will Account for Nearly Half of Connected Devices by 2020, Cisco Says*, ZDNet (June 7, 2016) (www.zdnet.com/article/iot-will-account-for-nearly-half-of-connected-devices-by-2020-cisco-says/).

[17] *Id.*

[18] *Who Makes the IoT Things Under Attack?*, Krebs on Security (Oct. 16, 2016) (krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/).

[19] *Webcams Involved in Dyn DDoS Attack Recalled,* TechCrunch (Oct. 24, 2016) (techcrunch.com/2016/10/24/webcams-involved-in-dyn-ddos-attack-recalled/).

[20] Federal Communications Commission, *Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order*, GN Docket No. 14-28, ¶ 105 (Rel. Mar. 12, 2015).

[21] *See id.* at ¶ 220.

[22] Center for Cyber & Homeland Security, Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats (Oct. 2016) (cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf).

[23] *See* 6 U.S.C. § 1503(a)-(c).

[24] *See id*.

state law. Accordingly, neither the FCC privacy rules nor the Electronic Communications Privacy Act[25] would prohibit or preclude ISPs from taking authorized actions for a cybersecurity purpose.

III. THE ROLE OF THE FEDERAL GOVERNMENT

The Federal Trade Commission (FTC) has also previously commented on the security risks posed by default passwords. In an August 2013 article on using IP cameras safely, the Commission encouraged consumers to change from the default username and password.[26]

In January 2015, the FTC released a staff report entitled, "Internet of Things: Privacy & Security in a Connected World."[27] The report summarized information presented at a FTC sponsored workshop and provided staff recommendations for ensuring privacy and cybersecurity in the IoT. Staff recommendations in the report included:

- Implement reasonable security
- Build-in security as part of the design of a product—not consider privacy or security risks after the fact
- Ensure personnel practices promote good security—provide training on security practices, only give access to consumers' personal data to personnel that need it, and designate personnel at an appropriate level within the company responsible for security.
- Retain service providers that are capable of maintaining reasonable security
- Implement a "defense-in-depth" approach with multiple levels of security, such as encrypting data
- Implement reasonable access control measures to limit the ability of unauthorized persons from access a consumer's product—such as limiting its ability to connect with certain other products
- Monitor products throughout their life cycle[28]

The National Telecommunications and Information Administration (NTIA) has initiated a multistakeholder process to review how best to approach security for IoT devices.[29] The National Institute of Standards and Technology (NIST) has also released an IoT security model

---

[25] *See* 18 U.S.C. § 2511(c).

[26] Federal Trade Commission, *Using IP Cameras Safely* (Aug. 2013) (www.consumer.ftc.gov/articles/0382-using-ip-cameras-safely).

[27] Federal Trade Commission, *Internet of Things: Privacy & Security in a Commercial World*, FTC Staff Report (Jan. 27, 2015).

[28] *Id.*

[29] National Telecommunications and Information Administration, *Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching* (Oct. 24, 2015) (www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security).

and is preparing to issue finalized standards for IoT security this week.[30] NIST officials have said they are releasing these finalized standards a month ahead of schedule in part because of the recent wave of IoT-based cyberattacks.[31] Similarly, some private groups have developed frameworks, which could be used to help standardize device security.[32] There are currently no federal requirements that mandate any level of security for IoT devices. Yet, there are currently no federal requirements that mandate any level of security for IoT devices.

IV. WITNESSES

The following witnesses have been invited to testify:

Dale Drew
Senior Vice President, Chief Security Officer
Level 3 Communications

Kevin Fu
Associate Professor, Department of Electrical Engineering and Computer Science
University of Michigan

Bruce Schneier
Adjunct Lecturer, Kennedy School of Government
Harvard University

---

[30] *NIST Develops Model for IoT Security*, FierceWireless (Aug. 1, 2016) (www.fiercewireless.com/tech/nist-develops-model-for-iot-security); *White House, NIST Prepare to Issue IoT Security Standards Ahead of DHS Guidance*, Inside Cybersecurity (Nov. 11, 2016) (insidecybersecurity.com/daily-news/white-house-nist-prepare-issue-iot-security-standards-ahead-dhs-guidance).

[31] *NIST Bumps up Release of Security Guidance*, GCN (Nov. 8, 2016) (gcn.com/articles/2016/11/08/nist-800-160-early-release.aspx).

[32] Online Trust Alliance, *Internet of Things* (otalliance.org/initiatives/internet-things) (accessed Nov. 8, 2016).