ENERGY & COMMERCE
CHAIR RODGERS

MEMORANDUM 01/09/2024

To: Members, Subcommittee on Communications and Technology
From: Majority Staff
Re: Communications and Technology Subcommittee Hearing

I. INTRODUCTION

On Thursday, January 11, 2024, at 10:00 a.m., the Subcommittee on Communications and Technology will hold a hearing in 2123 Rayburn House Office Building titled "Safeguarding Americans' Communications: Strengthening Cybersecurity in a Digital Era." The following witnesses are expected to testify:

II. WITNESSES

- Mr. Jim Richberg, Head of Cyber Policy, Fortinet
- Mr. Tobin Richardson, President and CEO, Connectivity Standards Alliance
- Mr. Clete Johnson, Senior Fellow, Center for Strategic & International Studies
- Mr. Alan Butler, Executive Director and President, Electronic Privacy Information Center

III. BACKGROUND

Each day, there are more than 2,200 cyberattacks on communications infrastructure in the United States, equating to nearly one attack every 39 seconds.[1] The communications industry is facing an increase in cyberattacks due to vulnerabilities in Internet of Things (IoT) devices and 5G networks and these attacks are aided by the use of artificial intelligence (AI). In January and February of 2023 alone, the data of 74 million U.S. telecom customers had already been leaked on the dark web.[2] The communications industry saw a 51 percent increase in the number of attacks in 2021, making it the third most targeted sector.[3] The increasing complexity of communications infrastructure combined with legacy networks provides criminals and malicious nation state actors a broad attack surface to exploit. With so many connected devices, communication networks are increasingly vulnerable to cyberattacks such as ransomware, phishing, distributed denial-of-service (DDoS) attacks, leading to significant breaches.[4]

[1] Jacob Fox, *Top Cybersecurity Statistics for 2024,* COBALT (Dec. 8, 2023), https://www.cobalt.io/blog/cybersecurity-statistics-2024#:~:text=According%20to%20Security%20Magazine%2C%20there,1%20cyberattack%20every%2039%20seconds.

[2] Sam Sabin, *Wave of telecom data breaches highlight industry's weakness,* AXIOS (Mar. 17, 2023), https://www.axios.com/2023/03/17/telecom-data-breaches-t-mobile-att.

[3] Check Point Research Team, *Check Point Research: Cyber Attacks Increased 50% Year over Year,* Check Point Software Technologies Ltd. (Jan. 10, 2022), https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year/.

[4] Dez Blanchfield, *Cybersecurity In The Telecommunications Industry,* https://elnion.com/2023/04/28/cybersecurity-in-the-telecommunications-industry-7-key-challenges/

IV. CYBERATTACKS

A cyberattack is an attempt by unauthorized users—including criminals, malicious nation state actors, or other digital adversaries –to access a computer network or system, usually for the purpose of altering, stealing, destroying, or exposing information.[5] Malware is any program or code created with the intent to do harm to a computer, network or server.[6] Malware includes ransomware, spyware, and worms, causing a variety of dangerous consequences. In ransomware attacks, an adversary encrypts a user's data and threatens to publish or delete the data until the ransom is paid. Ransomware is often disguised as legitimate software or hidden behind links in texts or emails.[7]

Phishing is the most common form of cybercrime, with an estimated 3.4 billion spam emails sent every day.[8] A phishing attack occurs when a malicious actor sends emails, texts, or other messages that camouflage themselves as trusted, legitimate sources in an attempt to grab sensitive information from the target. The bad actor may send a link that brings a user to a fake website, enticing a victim to share sensitive information — such as passwords or account numbers — or, by clicking the link, will covertly download malware to the target's device. Spear phishing, a more enhanced and targeted version of phishing, is a technique in which attackers collect information about the target, allowing them to tailor the phishing email or message, increasing their probability of success.[9] Similar to phishing, spoofing is a technique through which cybercriminals disguise themselves as a known or trusted source. In so doing, the adversary is able to engage with the target and access the target's systems or devices to reach the cybercriminal's ultimate goal.[10]

Adversaries are now also beginning to use AI to create new automated, aggressive, and coordinated attacks. Between January and February 2023, researchers observed a 135 percent increase in "novel social engineering" attacks, corresponding with the widespread adoption of ChatGPT. AI can be used to craft highly convincing phishing emails, create malware that adapts to security measures, and even automate the extraction of valuable data from compromised systems.[11]

V. INTERNET OF THINGS SECURITY

Over the past decade, IoT devices have become common household items. From the doorbell to the personal assistant in your living room, if it comes with power, it is likely

[5] Kurt Baker, *10 Most Common Types of Cyber Attacks,* CROWDSTRIKE (Nov. 9, 2023), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/.
[6] *Id.*
[7] *Id.*
[8] Charles Griffiths, *The Latest 2023 Phishing Statistics,* AAG IT SERVICES (Jan. 12, 2023), https://aag-it.com/the-latest-phishing-statistics/.
[9] *Baker, supra at 6.*
[10] *Id.*
[11] Gabriele Fiata, *Why Evolving AI Threats Need AI-Powered Cybersecurity,* FORBES (Oct. 4, 2023), https://www.forbes.com/sites/sap/2023/10/04/why-evolving-ai-threats-need-ai-powered-cybersecurity/?sh=35418e272edc.

connected to the Internet. IoT devices are remotely accessible by a user's personal device, such as a smartphone, via Wi-Fi, Bluetooth, or other connection type.[12] While this connectivity has many benefits, the ability to integrate multiple household items into a users' phone allows for the control of temperature, music, and security all from one central device.[13] As of early 2023, there are an estimated 15 billion connected IoT devices worldwide, with roughly 5 billion devices in the United States. This number is expected to double by 2030.[14]

The interconnected nature of these devices provides both a tremendous benefit and security weakness. As users add more IoT devices to their daily lives, this expands the attack surface that can allow a hacker to latch onto a network. With the inclusion of industrial IoT (IIoT) devices, enabling connection between information technology systems to operation technology systems, the importance of IoT security begins to intertwine with national security.[15] The device, the communications channels between IoT devices and connected devices, and any applications or software needed to operate the IoT device, become liabilities for both commercial and consumer use. The weak links allow malicious actors easy access to the rest of the internal network. This can extend to other connected IoT devices or personal devices on the network.

A group of IoT devices hacked by a single malicious actor can be formed into a botnet. This botnet can then be used to conduct distributed denial-of-service (DDoS) attacks against networks. DDoS attacks aim to disrupt services by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.[16] This disruption can impact millions of consumers, cause a shutdown of business operations, and result in significant financial losses.[17] Botnets have been used to attack hospitals,[18] financial institutions,[19] and political actors.[20] In 2016, the Subcommittees on Communication and Technology and Commerce, Manufacturing, and Trade held a hearing examining a series of IoT botnet attacks.[21] IoT vulnerabilities can also act as a

[12] Maggie Murphy, *Eight common IoT connectivity technologies & use cases,* HOLOGRAM (Jan. 4, 2022), https://www.hologram.io/blog/iot-connectivity-technologies/.

[13] Emma Crockett, *85 Top IoT Devices*, DATAMATION (Apr. 26, 2023), https://www.datamation.com/mobile/85-top-iot-devices/.

[14] Fabio Duarte, *Number of IoT Devices (2023),* EXPLODING TOPICS (Feb. 22, 2023), https://explodingtopics.com/blog/number-of-iot-devices.

[15] *Industrial Internet of Things (IIoT),* TREND MICRO (accessed Dec. 19, 2023), https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot.

[16] *What is a DDoS Attack?* Cloudflare (accessed Dec. 19, 2023), https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

[17] Baker, *supra* note *6.*

[18] Jonathan Greig, *CISA says Killnet DDoS attacks on U.S. hospitals had little effect,* THE RECORD (Feb. 7, 2023), https://therecord.media/ddos-hospitals-cisa-killnet-limited-effects.

[19] Jessica Lyons Hardcastle, *Huge DDoS attack against US financial institution thwarted,* THE REGISTER (Sep. 11, 2023), https://www.theregister.com/2023/09/11/ddos_attack_against_us_bank/.

[20] Stephen Weigand, *FBI Warns of politically motivated hacktivist activity, DDos attacks in alert,* SC MEDIA (Nov. 7, 2022), https://www.scmagazine.com/news/fbi-warns-of-politically-motivated-hacktivist-activity-ddos-attacks-in-alert.

[21] *#SubCommTech and #SubCMT Examine Recent Cyber Attack*, HOUSE ENERGY AND COMMERCE COMMITTEE PRESS RELEASE (Nov. 16, 2016), https://energycommerce.house.gov/posts/subcommtech-and-subcmt-examine-recent-cyber-attacks.

gateway into deeper, more secure parts of a network.[22] Finally, due to the uses of these technologies, simply accessing the software within the device itself can wreak havoc.[23]

A. Chinese Communist Party (CCP) Influence in IoT Cellular Modules

Cellular modules are components within IoT devices that enable connectivity to the Internet. As IoT devices are often designed to be operated remotely, the importance of this connection cannot be understated. The Committee has taken direct action to limit the pervasiveness of CCP in U.S. communications networks. This includes passing the Secure and Trusted Communications Networks Act, which placed foreign adversary-controlled companies, such as Huawei and ZTE Corporation, under severe sanction against participation in U.S networks.[24] Unfortunately, the influence of the CCP has found itself back inside our systems through IoT cellular modules. Companies like Quectel and Fibocom, whose websites states that people using Fibocom's Platform "shall comply with…the laws of the People's Republic of China," represent serious threats to U.S. national security.

VI. ADMINISTRATION ACTIONS

A. U.S. Cyber Trust Mark

On August 10, 2023, the Federal Communication Commission (FCC) released a notice of proposed rulemaking seeking to create a voluntary cybersecurity labeling program for IoT devices.[25] The FCC relied upon its equipment authorization authority to adopt the proposed labeling program.[26] This program, named the U.S. Cyber Trust Mark, would provide a voluntary certification for IoT devices.

IoT devices that qualify for certification will be permitted to use the Commission' new distinctive label, representing their participation and compliance with a set of standards. These standards will be based on work product from the National Institute for Standards and Technology (NIST), including NIST's whitepaper, "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products."[27] Once the program is in place, qualifying products bearing the U.S. Cyber Trust Mark would need to maintain the product in order to remain a lawful displayer of the trademarked label. A third-party administrator would manage the U.S. Cyber Trust Mark and update the database of products labeled with the mark. The FCC parallels this program to the Energy Star program.[28]

[22] Iain Thomson, *Wi-Fi baby heart monitor may have the worst IoT security of 2016,* THE REGISTER (Oct. 13, 2016), https://www.theregister.com/2016/10/13/possibly_worst_iot_security_failure_yet/.

[23] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It,* WIRED (Jul. 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[24] Secure and Trusted Communications Networks Act of 2019, P.L. 116-124 (2020), *codified at* 47 U.S.C. 1601, et seq.

[25] *In the Matter of Cybersecurity Labeling for Internet of Things*, FEDERAL COMMUNICATIONS COMMISSION, Notice of Proposed Rulemaking (Aug. 6, 2023), https://docs.fcc.gov/public/attachments/FCC-23-65A1.pdf.

[26] 47 U.S.C §302(a).

[27] *See, e.g.,* NIST, Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products at 3-10 (2022), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf.

[28] *About Energy Star,* (accessed Dec. 19, 2023), https://www.energystar.gov/about.

B. Executive Order 14028: Improving the Nation's Cybersecurity

On May 12, 2021, President Biden issued an Executive Order (EO) on "Improving the Nation's Cybersecurity".[29] It was created in response to the growing number of cyberattacks launched against government agencies, critical infrastructure, and private companies based in the U.S. The EO aims to help both the U.S. government and the private sector better protect themselves against cyber threats. The EO establishes a framework that explains how to improve cybersecurity in the U.S. and specifies the technologies and practices required for this purpose. Specifically, the EO requires organizations to implement three cybersecurity measures: 1) secure development processes to prevent supply chain attacks, 2) scan application code to ensure it is secure, 3) create a software bill of materials to identify if there are vulnerable components used within a software application.[30]

C. National Cybersecurity Strategy

In March 2023, the Biden administration issued a National Cybersecurity Strategy to defend against cyber-threats and invest in cybersecurity solutions. The strategy outlines five pillars to support the nation's cybersecurity: 1) defend critical infrastructure, 2) disrupt and dismantle threat actors, 3) shape market forces to drive security and resilience, 4) invest in a resilient future, and 5) forge international partnerships to pursue shared goals.[31]

D. FCC E-Rate Expansion

On December 29, 2023, the FCC released a proposed rule for the Schools and Libraries Cybersecurity Pilot Program. This program would expand the Universal Service Fund's (USF) E-Rate program, providing $200 million to eligible K-12 schools and libraries for the procurement of eligible cybersecurity services.[32] This proposed rule comes after the Commission approved a Notice of Proposed Rulemaking regarding the program on November 8, 2023.[33]

VII. CHINESE-MANUFACTURED INFRASTRUCTURE

On Mach 12, 2020, Congress enacted the Secure and Trusted Communications Networks Act (STCNA) of 2019.[34] The law prohibits a recipient of the FCC's Universal Service Fund (USF) from purchasing, obtaining, or maintaining any equipment or services from companies posing a national security threat, and requires the FCC to publish a list of "covered communications equipment or services" within one year that pose such a threat. The law also

[29] Improving the Nation's Cybersecurity, 86 Fed. Reg. 26633 (Mar. 17, 2023), https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

[30] *Id.*

[31] *National Cybersecurity Strategy,* THE WHITE HOUSE (Mar. 1, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[32] School and Libraries Cybersecurity Pilot Program, 88 Fed. Reg. 90141 (Dec. 29, 2023), https://www.federalregister.gov/documents/2023/12/29/2023-27811/schools-and-libraries-cybersecurity-pilot-program.

[33] *In the Matter of Schools and Libraries Cybersecurity Pilot Program,* FEDERAL COMMUNICATIONS COMMISSION, Notice of Proposed Rulemaking (Nov. 8, 2023), https://docs.fcc.gov/public/attachments/FCC-23-92A1.pdf.

[34] STCNA, *supra* note 28.

established a program to reimburse certain eligible communications providers for replacing covered communications equipment or services. Through the Consolidated Appropriations Act, 2021, Congress provided $1.9 billion to the FCC for the reimbursement program.[35]

In July 2022, the FCC announced that it approved applications from providers requesting a total of $4.98 billion to fund all reasonable and supported cost estimates and administrative expenses for the program—a shortfall of $3.08 billion.[36] Absent additional appropriations, the FCC plans to pro-rate each applicant's allocation by 39.5 percent.[37] As of October 2, 2023, reimbursement claim requests have been submitted for 122 of the 126 approved applicants, and these providers have one year from when they submitted their first reimbursement claim to remove untrusted equipment, resulting in deadlines ranging from October 8, 2023, to September 23, 2024.[38] The FCC has approved several requests to extend these deadlines by six months due to the funding shortfall.[39]

VIII. BORDER GATEWAY PROTOCOL

Border Gateway Protocol (BGP) enables the internet to exchange routing information between autonomous systems (AS).[40] BGP is like a postal service for the internet. It ensures that the mail, or network packets, makes it to the intended destination in as few steps as possible. BGP is able to scan the available options before deciding which route is the quickest and most efficient route for delivery, requiring coordination between multiple BGP speakers at once. An AS will announce its routes and the destinations reachable from its system.[41] These BGP announcements are then kept and managed by an Internet Routing Registry (IRR) system. IRR systems are managed by several regional and global entities.[42] The coordination of these systems allows for the internet to operate as it does today.

The current version of BGP lacks authentication and integrity mechanisms that would intentionally authorize an AS to make BGP announcements only when necessary and only when validated. This leads to vulnerabilities such as prefix hijacks, which allow for the alteration of packet destination; route hijacks, changing the route to pass through an unintended AS controlled by malicious actors; and route leaks, providing an in-depth look into the routing characteristics of the selected AS.

[35] Consolidated Appropriations Act, 2021 § 906(2).
[36] Letter from Jessica Rosenworcel, Chair, FCC, to Sen. Maria Cantwell et al. (July 15, 2022), https://docs.fcc.gov/public/attachments/DOC-385335A1.pdf.
[37] *Id.*
[38] Letter from Jessica Rosenworcel, Chair, FCC, to Sen. Maris Cantwell et al. (Oct. 10, 2023), https://docs.fcc.gov/public/attachments/DOC-397596A1.pdf.
[39] *Id.*
[40] *What is BGP? | BGP Routing Explained* (accessed Dec. 12, 2023), https://www.cloudflare.com/learning/security/glossary/what-is-bgp/.
[41] *What is Border Gateway Protocol and BGP announcements?,* BIGDATA CLOUD (accessed Dec. 12, 2023), https://www.bigdatacloud.com/support/what-is-bgp.
[42] Alessandro Improta and Luca Sani, *How BGP Routing Really Works*, CATCHPOINT (Oct. 24, 2019), https://www.catchpoint.com/blog/bgp-routing.

In 2008, Pakistan accidentally shutdown worldwide access to YouTube when attempting to restrict its own citizens from accessing the website.[43] As a part of this effort, the Internet Service Provider (ISP) for Pakistan created a fake route that discarded YouTube traffic instead of delivering the request to its final destination. The Pakistani company accidentally made a BGP announcement for this fake route to a partner network in Hong Kong, who in turn announced this new route to the world. 97 major ISPs and thousands of smaller providers routed the traffic intended for YouTube into Pakistan's newly created BGP blackhole. For nearly two hours, an unknown number of users were unable to access YouTube.

IX. KEY QUESTIONS

- What are the most prevalent cybersecurity vulnerabilities in modern telecommunications networks?
- Are there specific emerging threats or attack vectors that experts believe pose a significant risk to the industry in the near future?
- In what ways are adversary nation-states involved in cyberattacks targeting telecommunications infrastructure?
- In the event of a cybersecurity incident, what best practices and frameworks should telecommunications companies follow in terms of incident response and recovery?

X. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Kate O'Connor, Giulia Leganski, or Slate Herman of the Committee Staff at (202) 225-3641.

[43] Brad Stone, *Pakistan Cuts Access to YouTube Worldwide,* NEW YORK TIMES (Feb. 26, 2008), https://www.nytimes.com/2008/02/26/technology/26tube.html.