ELIJAH E. CUMMINGS, MARYLAND
CHAIRMAN

ONE HUNDRED SIXTEENTH CONGRESS

JIM JORDAN, OHIO
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5051
MINORITY (202) 225–5074

http://oversight.house.gov

MEMORANDUM

September 4, 2019

To: Members of the Subcommittee on National Security

Fr: Committee Staff

Re: Hearing on "Securing the Nation's Internet Architecture"

On **Tuesday, September 10, 2019, at 2:00 p.m., in room 2118 of the Rayburn House Office Building**, the House Committee on Armed Services Subcommittee on Intelligence, Emerging Threats and Capabilities and the House Committee on Oversight and Reform Subcommittee on National Security will hold an open hearing on how departments and agencies across the federal government coordinate to secure the critical components and locations upon which the nation's internet architecture depends. The hearing will also allow members to assess and examine the policies, authorities, and guidance for departments and agencies to collaborate, synchronize, and deconflict efforts.

I. OBJECTIVES FOR THE HEARING

- Examine relevant Executive Branch departments and agencies' roles and responsibilities in securing internet architecture, particularly at the data link and physical layers of internet connectivity.

- Ensure that departments and agencies have harmonized and deconflicted programs and policies aimed at internet security, to particularly include engagement between security-focused and non-security-focused departments and agencies (e.g. Department of Defense and Department of Commerce).

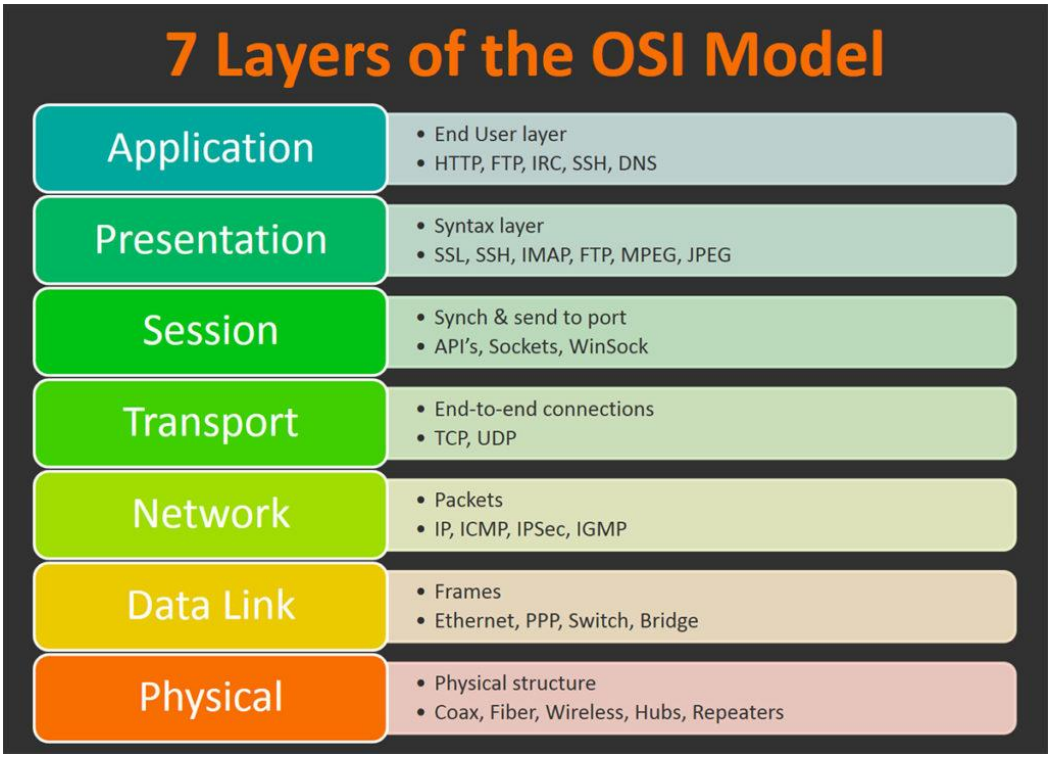
- Encourage a whole-of-government approach to securing internet architecture, vice the current practice of dividing responsibilities among departments and creating stovepipes and seams in jurisdictions.

- Understand the level of the federal government's preparedness against an attack with both cyber and physical components.

II. KEY BACKGROUND REGARDING INTERNET INFRASTRUCTURE AND AGENCY ROLES IN SECURING THIS ARCHITECTURE

The internet is both ubiquitous and essential to everyday life and national economic livelihood. U.S. citizens rely on the internet to access medical care and private data, engage in interstate and international commerce, and enable highly optimized manufacturing and trade. Increased wireless connectivity in the United States is positively correlated with national economic growth, and by 2011, the internet had already accounted for 3.4% of the nation's Gross Domestic Product.[1] The internet is enabled by a diverse set of hardware, software, protocols, switches, routers, fiber, and other components that must operate for individuals to be able to access their email, bank statements, and business.

Conceptually, the internet can be explained through the Open Systems Interconnection (OSI) model, a framework that characterizes how information flows between systems and devices. The graphic below explains the seven layers of the OSI model and provides examples of the technologies and equipment that comprise each layer.



Most internet users are familiar with the seventh, or application layer. These are the programs and applications that individuals keep on their phones, tablets, and laptops to access information and data. As one moves from top to bottom on the model, the technologies become

[1] *The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity.*, McKinsey Global Institute (2011) (Accessed Aug. 25, 2019) (online at www.mckinsey.com/~/media/McKinsey/Industries/High%20Tech/Our%20Insights/The%20great%20transformer/MGI_Impact_of_Internet_on_economic_growth.ashx) .

less focused on the end user, and more about the broader base of users, or written another way, from the phone to the owners and operators of the telecommunications systems.

The internet as a resource and a system of systems is primarily built, funded, owned, and operated by the private sector. Private businesses host their own networks, build their own sites, and rely on others to provide services such as security and advertising. The largest Internet Service Providers (ISPs) are generally publicly-traded companies, while those smaller and more regionally focused are privately-held entities. While no entity owns the internet, there are several non-governmental, international entities which play an outsized role in governing the internet, such as The Internet Society, the Internet Engineering Task Force, and the Internet Corporation for Assigned Names and Numbers (ICANN).

Within the United States, unlike other countries, the government does not manage the internet, nor direct its use, but rather sets the laws, policies, and procedures for the private sector, academia, and individuals to follow in their use of the internet. In some key ways, the internet as a public good is comparable to a utility company supplying electricity to a community, with the government issuing regulations, while the operations are run by a utility company. From a national security perspective, securing the nation's internet architecture requires engagement with private sector partners due to how much this architecture is privately owned and operated.

Due to its decentralized nature, however, no single government agency or entity is responsible for maintaining the security and reliability of the internet. In addition, the proper functioning of the internet is heavily dependent on an implicit level of trust between the various public and private entities who own or oversee its myriad components. In a November 18, 2016, report, the Congressional Research Service (CRS) noted:

> First, the internet is inherently international and cannot in its totality be governed by national governments whose authority ends at national borders. Second, the internet's successful functioning depends on the willing cooperation and participation by mostly private sector stakeholders around the world.[2]

More recently, in a July 8, 2019, report, CRS noted this meant critical infrastructure protection "remains a highly distributed enterprise that competes for limited resources with other priorities across the federal government." The report also stated that critical infrastructure security in the U.S. Government "has evolved into a distributed enterprise loosely structured by institutionalized partnerships and policy frameworks."[3] In addition to the private sector, the federal agencies and departments responsible for the security and resiliency of U.S. internet architecture include the Department of Homeland Security (DHS), the Department of Defense (DOD), and the Department of Commerce, among others.

---

[2] Congressional Research Service, *Internet Governance and the Domain Name System: Issues for Congress* (Nov. 18, 2016) (online at www.crs.gov/reports/pdf/R42351).

[3] Congressional Research Service, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress* (July 8, 2019) (online at https://fas.org/sgp/crs/homesec/R45809.pdf).

A. Department of Homeland Security

DHS is the Sector-Specific Agency for both the Communications and Information Technology sectors. The Cybersecurity and Infrastructure Agency (CISA), which Congress created through the "Cybersecurity and Infrastructure Security Agency Act of 2018" (*Public Law 115-278),* is a DHS operational component that has primary responsibility for coordinating with other federal departments and agencies, state, local, tribal, and territorial (SLTT) entities, and the private sector, to protect U.S. critical infrastructure from cyber- and physical-related threats. CISA is also responsible for issuing emergency communications, providing guidance, and conducting outreach efforts to these other entities in the pursuit of protecting U.S. critical infrastructure.

B. Department of Defense

DOD is responsible for defending the nation from attacks, to include attacks against U.S. critical infrastructure both in the physical and cyber domains. The Office of the Deputy Assistant Secretary of Defense for Cyber Policy has jurisdiction over establishing and implementing DOD's cyberspace policies and strategies related to cyberspace.

In its 2018 Cyber Strategy, DOD said it would conduct cyberspace operations to maintain U.S. military advantages, defend national interests, collect intelligence, and "prepare military cyber capabilities to be used in the event of crisis or conflict." DOD further stated it would seek to prevent and stop "malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact" DOD directly. DOD's strategy also states that the Department will work with the U.S. interagency, U.S. allies, and international partners to enforce responsible cyberspace behavior during peacetime.[4]

C. Department of Commerce

The Department of Commerce has jurisdiction over telecommunications and internet infrastructure through the National Telecommunications and Information Administration (NTIA). NTIA coordinates and develops executive branch policies related to telecommunications and information systems.

NTIA is responsible for monitoring the security and permanency of the internet's Domain Name System (DNS) and internet protocol (IP) address system, which are core components of internet architecture. From 1998 until September 2016, NTIA maintained a contract with ICANN for the coordination and management of the DNS and IP addresses. This contract gave NTIA a more direct oversight role over these systems and ICANN. As of September 2016, NTIA no longer maintains this contract, but continues to have an advisory role with respect to ICANN, in conjunction with international partners.

[4] Department of Defense, *2018 Department of Defense Cyber Strategy* (Sept. 18, 2018) (online at https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF)

D. Other U.S. Government Entities

Multiple other departments and agencies, as well as the White House, have jurisdiction over U.S. cybersecurity policy and protecting internet architecture. These include, but are not limited to:

- The Executive Office of the President, which is responsible for developing policy, creating national-level strategies related to security and defense, and implementing these policies through various mechanisms, including the National Security Council and the Office of Management and Budget.

- The Federal Communications Commission, which under PPD-21, is required to use its regulatory authority to prioritize the security of communications infrastructure, identify vulnerabilities in this infrastructure, and work with public- and private-sector partners to remove these vulnerabilities.

- The Department of Energy serves as the sector-specific agency for the electric sector, essential in keeping the telecommunications sector running. The department also operates multiple National Laboratories that conduct research and development activities related to cybersecurity.

- The Department of Justice, which is responsible for enforcing federal laws, carrying out investigations, and prosecuting criminal violations related to cybersecurity.

- The Intelligence Community, which provides various intelligence assessments regarding threats to critical infrastructure.

E. The Private Sector

ISPs are responsible for providing internet to businesses and homes, as well as moving internet traffic around the world to other ISPs. While there are more than 2,600 ISPs in the U.S., the top 10 ISPs deliver internet to the overwhelming majority of Americans.[5] ISPs are broadly categorized into three tiers. These are meant to distinguish between the top tier, or Tier 1, providers that are the largest, most systemically important entities that run networks moving immense amounts of internet traffic and the smaller ISPs that move traffic to consumers in particular parts of states or cities.

In simplified terms, Tier 1 providers move internet traffic between continents and countries. Tier 2 providers are intermediaries that move traffic from the larger intercontinental networks closer to the consumers. Finally, Tier 3 providers are those that are responsible for the "last mile" of data transmission, from the large networks to individual homes and businesses.

[5] *"Internet Providers in the U.S."*, BroadBandNow (Accessed on Aug. 25, 2019) (online at https://broadbandnow.com/All-Providers).

To facilitate communications among ISPs in a given area or between countries and continents, ISPs depend on large volume assets: Internet Exchange Points (IXPs) and optical fiber cables. While most Americans receive internet on their end-user devices through wireless means (WiFi, cell sites), most data are transmitted through optical fiber cables. IXPs are the physical locations where ISPs' traffic is exchanged and bulk traffic is routed towards its ultimate destination. IXPs are generally owned and operated by either non-profit consortiums or neutral specialty businesses. In the case of the U.S., there are only 139 IXPs servicing the entire country, and disruptions can result in significant impacts to a given area.

III. CRITICAL INFRASTRUCTURE IN THE U.S. GOVERNMENT

The United States has wrestled with the challenge of defending critical infrastructure for decades. The current schema is based on the February 2013 Presidential Policy Directive 21 (PPD-21) titled, "*Critical Infrastructure and Resilience*." PPD-21 acknowledged that protection of U.S. critical infrastructure, including communications systems and internet infrastructure, is "a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure."[6] PPD-21 established 16 critical infrastructure sectors and designated an SSA to act as the lead coordinator for each sector. Of the 16 critical infrastructure sectors, three specifically apply to internet infrastructure and architecture: Communications, Information Technology, and Electricity.

While PPD-21 designated primary responsibility for protecting the nation's critical infrastructure to DHS and the Secretary of Homeland Security, this did not give DHS unilateral control or jurisdiction over defending critical infrastructure. In the case of internet architecture, the overlap in jurisdictions is complex. For example, while DHS is responsible for protecting critical infrastructure, the DOD is the only federal entity charged with defending the United States from attacks on civilian infrastructure and the undersea cables linking the U.S. to other countries.

The complexity of overlapping mandates and jurisdictions has led departments and agencies to focus narrowly on discrete components or pieces of securing internet architecture, however, this approach overlooks the nature of the internet as a single ecosystem or system of systems, which given its' importance to the nation, requires dedicated attention.

IV. POTENTIAL THREATS TO INTERNET ARCHITECTURE

In a June 2006 report, the Government Accountability Office stated that global internet infrastructure is at risk of "disruptions in service due to terrorist and other malicious attacks, natural disasters, accidents, technological problems, or a combination of the above." These

[6] The White House, *Presidential Policy Directive – Critical Infrastructure Security and Resilience* (Feb. 12, 2013) (online at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil).

disruptions can be caused by "cyber and physical incidents – both intentional and unintentional."[7]

The U.S. sector-specific plans for the Communications and Information Technology critical infrastructure sectors describe a variety of threats to both sectors. The Information Technology Sector-Specific Plan states the sector "faces cyber and physical dangers at the hands of criminals, hackers, terrorists, and nation-states."

> Manmade threats have rapidly evolved from physical sabotage and simple automated worms and viruses, to complex social engineering attacks that exploit known and unknown vulnerabilities in IT products and services.[8]

The Communications Sector-Specific Plan describes four main areas of risk for the sector, including natural disasters and extreme weather, supply chain vulnerabilities, cyber vulnerabilities, and geopolitical instability. These risk areas include threats and vulnerabilities that can be exposed through accidental and natural events, or intentional malign activity.[9]

Recent incidents demonstrate the potential threats and vulnerabilities to U.S. internet architecture. For example, on January 22, 2019, the DHS Cybersecurity and Infrastructure Agency (CISA) issued Emergency Directive 19-01, which warned federal agencies about a global DNS hijacking campaign that included attackers redirecting and intercepting web and mail traffic. According to CISA, the campaign affected domains owned by multiple Executive Branch agencies.[10] U.S. military officials have also noticed increased Russian submarine activity around undersea data cables in the Atlantic Ocean, warning that this activity could indicate attempts to monitor, cut, or interfere with the cables.[11]

V. WITNESSES

Ms. Jeanette Manfra
Assistant Director for Cybersecurity
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

---

[7] Government Accountability Office, *Internet Infrastructure: Department of Homeland Security Faces Challenges in Developing a Joint Public/Private Recovery Plan* (June 16, 2006) (online at www.gao.gov/products/GAO-06-672).

[8] Department of Homeland Security, *Information Technology Sector-Specific Plan: An Annex to the NIPP 2013* (2016) (online at www.dhs.gov/publication/nipp-ssp-information-technology-2016).

[9] Department of Homeland Security, *Communications Sector-Specific Plan: An Annex to the NIPP 2013* (2015) (online at www.dhs.gov/publication/nipp-ssp-communications-2015).

[10] Department of Homeland Security, *Emergency Directive 19-01* (Jan. 22, 2019) (online at https://cyber.dhs.gov/ed/19-01/).

[11] *Russian Submarines Are Prowling Around Vital Undersea Cables. It's Making NATO Nervous.*, Washington Post (Dec. 22, 2017) (online at www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html).

Mr. B. Edwin "Ed" Wilson
Deputy Assistant Secretary of Defense for Cyber Policy
Office of the Undersecretary of Defense for Policy
Department of Defense

Ms. Diane Rinaldo
Acting Assistant Secretary and Administrator
National Telecommunications and Information Administration
Department of Commerce

Staff contacts: Matt Patane, Dan Rebnord, Michael Koren, and Kyle Smithwick at (202) 225-5051.