[H.A.S.C. No. 116–43]

SECURING THE NATION'S INTERNET ARCHITECTURE

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES

MEETING JOINTLY WITH THE

SUBCOMMITTEE ON NATIONAL SECURITY

OF THE

COMMITTEE ON OVERSIGHT AND REFORM

[Serial No. 116–57]

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

HEARING HELD
SEPTEMBER 10, 2019

U.S. GOVERNMENT PUBLISHING OFFICE
40–505 WASHINGTON : 2020

COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

JAMES R. LANGEVIN, Rhode Island, *Chairman*

RICK LARSEN, Washington
JIM COOPER, Tennessee
TULSI GABBARD, Hawaii
ANTHONY G. BROWN, Maryland
RO KHANNA, California
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
CHRISSY HOULAHAN, Pennsylvania
JASON CROW, Colorado, *Vice Chair*
ELISSA SLOTKIN, Michigan
LORI TRAHAN, Massachusetts

ELISE M. STEFANIK, New York
SAM GRAVES, Missouri
RALPH LEE ABRAHAM, Louisiana
K. MICHAEL CONAWAY, Texas
AUSTIN SCOTT, Georgia
SCOTT DesJARLAIS, Tennessee
MIKE GALLAGHER, Wisconsin
MICHAEL WALTZ, Florida
DON BACON, Nebraska
JIM BANKS, Indiana

Josh Stiefel, *Professional Staff Member*
Peter Villano, *Professional Staff Member*
Caroline Kehrli, *Clerk*

COMMITTEE ON OVERSIGHT AND REFORM

SUBCOMMITTEE ON NATIONAL SECURITY

STEPHEN F. LYNCH, Massachusetts, *Chairman*

JIM COOPER, Tennessee
PETER WELCH, Vermont
HARLEY ROUDA, California
DEBBIE WASSERMAN SCHULTZ, Florida
ROBIN L. KELLY, Illinois
MARK DeSAULNIER, California
STACEY E. PLASKETT, Virgin Islands
BRENDA L. LAWRENCE, Michigan

JODY B. HICE, Georgia, *Ranking Minority Member*
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
MARK MEADOWS, North Carolina
MICHAEL CLOUD, Texas
MARK E. GREEN, Tennessee
CLAY HIGGINS, Louisiana

Dave Rapallo, *Staff Director, Committee on Oversight and Reform*
Dan Rebnord, *Staff Director, Subcommittee on National Security*
Amy Stratton, *Clerk*

CONTENTS

Page

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

Prepared Statements:

Documents Submitted for the Record:

[There were no Documents submitted.]

Witness Responses to Questions Asked During the Hearing:

Questions Submitted by Members Post Hearing:

SECURING THE NATION'S INTERNET ARCHITECTURE

HOUSE OF REPRESENTATIVES, COMMITTEE ON ARMED SERVICES, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES, MEETING JOINTLY WITH THE COMMITTEE ON OVERSIGHT AND REFORM, SUBCOMMITTEE ON NATIONAL SECURITY, *Washington, DC, Tuesday, September 10, 2019.*

The subcommittees met, pursuant to call, at 2:01 p.m., in room 2118, Rayburn House Office Building, Hon. James R. Langevin (chairman of the Subcommittee on Intelligence and Emerging Threats and Capabilities) presiding.

OPENING STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, CHAIRMAN, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES, COMMITTEE ON ARMED SERVICES

Mr. LANGEVIN. The subcommittee will come to order.

So, good afternoon, everyone. I am pleased to welcome everyone here today to the joint hearing with the Committee on Oversight and Reform Subcommittee on National Security about the security of the Nation's internet architecture. I am particularly thankful to my good friend Congressman Lynch from Massachusetts, my neighbor in New England, and his staff for working so diligently in making today possible, along with the ranking members of both subcommittees.

Today we are here to conduct what I believe is much-needed oversight regarding the security of the internet's underlying architecture, namely, the components, physical sites, and the assets that are necessary for the internet to operate.

Defending the United States assets in this global telecommunications network requires a whole-of-government approach, and I am concerned that the government is not approaching the subject in a cohesive or comprehensive manner, creating significant risk for the Nation.

Both the Oversight subcommittee and the Armed Services subcommittee are seeking a better understanding of the policies, regulations, and guidelines and interagency agreements that govern the protection of this critical infrastructure. To the extent that there are gaps, we are also interested in learning whether legislative solutions may be needed.

Most people think of the internet as the sites they visit, the applications they use, and the emails they send. In other words, the people's understanding of what the internet is, is very much tied to how they engage with it. However, this leaves out an entire architecture that enables the flow of information around the world and into people's palms. This architecture includes the high-capacity cables buried under the ground and laid below the sea, the cable landing stations that connect the cables from continent to continent, and the internet exchange points, or IXPs, that serve as a clearinghouse for data between internet service providers and content delivery networks. These are all examples of physical sites and tangible items that are required for the internet to operate effectively.

While these physical sites are critical components of the cyber landscape, they are generally viewed as distinct from the network's protocols and software that are more familiar to people's understanding of the internet. However, they are just as important to internet operations. After all, unplugging a network cable is just as effective as a denial-of-service attack, maybe even more so.

From the government's perspective, attacking the subject of internet architecture security is difficult, due to the departments' and agencies' overlapping jurisdictions, responsibilities, and capabilities. And I am concerned that the executive branch has fragmented internet architecture security among multiple departments as opposed to conceptualizing the internet as a single ecosystem with departments working collaboratively.

For example, the Department of Homeland Security serves as the government lead for all critical infrastructure, and as the sector-specific agency for the telecommunications sector. Meanwhile, the Department of Commerce's National Telecommunications and Information Administration, or NTIA, is principally responsible for advising the President on telecommunications and information policy issues, and develops national policies on internet use and cybersecurity.

Separately, the Department of Defense is broadly responsible for defense of the Nation. Independent regulatory agencies, like the Federal Communications Commission, also have important responsibilities for ensuring security. To top it all off, many of these exchange points are connected to international providers.

So I have no doubt that these agencies work together broadly. However, I am very worried that by carving out discrete lanes in the road, there are seams left unaddressed in the middle, and I am concerned that internet architecture security is one of those seam issues.

Holistic internet architecture security has been generally neglected, I believe, with organizations remaining firmly in their lanes rather than approaching the problem collectively. So, for example, the Department of Homeland Security serves as the government lead for—so, in any event, separately, the Department of Defense—and DOD [Department of Defense] is broadly responsible for defense of the Nation.

Our Nation's newest cybersecurity organization, the Cybersecurity and Infrastructure Security Agency, has recognized the inherent challenges in using the critical sector framework, particularly with respect to interdependencies between sectors.

The National Risk Management Center's National Critical Functions Set explicitly recognizes internet architecture functions, such as "Operate Core Network" and "Provide Internet Routing, Access, and Connection Services." I am hopeful that this new framing will help stimulate more cross-agency and cross-sector discussion, interaction, and policy development.

So the purpose of today's hearing is to better understand how the interagency is approaching internet architecture security, including with respect to engagement with the private sector. In particular, I will be interested in hearing from the witnesses how their agencies deal with the fact that internet architecture security is not purely a cyber problem and it is not a purely physical problem. In order to effectively reduce our risks, DOD will have to engage actively and eagerly non-security-centric agencies such as NTIA and regulatory bodies such as the Federal Communications Commission, and vice versa.

Our country's cyber experts will have to sit down with specialists in physical security and electrical distribution professionals, because at the end of the day, it won't matter if these sites and systems are taken offline by cyberattack, sabotage, or natural disaster.

There is no greater sign of how cross-cutting this issue is than the fact that the IETC [Intelligence and Emerging Threats and Capabilities] Subcommittee is joined today by the Oversight Committee's National Security Subcommittee. Even within the House of Representatives, we are inclined to handle things within caucuses or within committees; but in recognition of the problem's scale, we are here today tackling this issue together, because that is exactly what it will take at the end of the day.

So, with that, and before turning to the Ranking Member Stefanik and then to Chairman Lynch and Ranking Member Hice, let me take a minute just to introduce today's witnesses.

Ms. Jeanette Manfra serves as the inaugural Assistant Director for Cybersecurity with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency [CISA]. Ms. Manfra served as Assistant Secretary with the Office of Cybersecurity Communications at CISA's predecessor organization, the National Protection and Programs Directorate, before assuming her current role. Ms. Manfra has held numerous other roles within DHS [Department of Homeland Security], and she has also served on the National Security Council staff. Before joining DHS, Ms. Manfra served in the U.S. Army as a communications specialist and as a military intelligence officer. I have known Jeannette now for several years, and I have great confidence in her and Director Krebs' leadership at CISA.

Joining us also today we have Deputy Assistant Secretary of Defense for Cyber Policy, Mr. Ed Wilson. In his capacity as the director of—in his capacity, he supports the Secretary of Defense and other senior leaders by formulating, recommending, integrating, and implementing policies and strategies to improve DOD's ability to operate in cyberspace. Prior to this duty, General Wilson retired from the United States Air Force after serving on Active Duty for over 32 years, to include the triple-hatted role of Commander, 24th Air Force; Commander, Air Forces Cyber; and Commander, Joint Force Headquarters-Cyber. Welcome, and General, thanks for your service.

And finally, Ms. Diane Rinaldo is the Acting Assistant Secretary for Communications and Information for the Department of Commerce and the Administrator of the National Telecommunications and Information Administration. Ms. Rinaldo also serves as the Deputy Assistant Secretary for Communications and Information. I have closely tracked several of NTIA's cybersecurity initiatives, including on cybersecurity vulnerabilities, disclosure and software component transparency, and I appreciate her continued support in that agency for multi-stakeholder processes to improve internet security. I will also note that Ms. Rinaldo is a proud veteran of the House Permanent Select Committee on Intelligence, where she and I worked before, where she served as the lead committee staffer on our information-sharing legislation, the Cybersecurity Act of 2015.

So I welcome all of our witnesses today. And, with that, I want to turn to Ranking Member Stefanik for any comments that she may have.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 43.]

STATEMENT OF HON. ELISE M. STEFANIK, A REPRESENTATIVE FROM NEW YORK, RANKING MEMBER, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES, COMMITTEE ON ARMED SERVICES

Ms. STEFANIK. Thank you, Jim. I want to start by thanking both Chairman Langevin and Chairman Lynch for holding such an important and cross-cutting hearing. I am also pleased to be here with my fellow ranking member, Mr. Hice.

We are fortunate that we are joined by such an excellent interagency panel of witnesses to guide us today. Ms. Manfra, it is great to see you again before this committee. When last we spoke, it was regarding election security, and I am pleased that today's hearing will span many of the other important missions of your organization, the CISA.

Ms. Rinaldo, given the important role that NTIA plays, we are fortunate to have you here as well. And since, as the chairman mentioned, you are a former professional staff member from HPSCI [House Permanent Select Committee on Intelligence], we can say welcome back to the House.

And, Mr. Wilson, it is always great to see you back before the subcommittee. We look forward to hearing how the Department of Defense supports these agencies and our broader national security objectives.

As we look to further improve the security of our Nation's internet architecture, we should remind ourselves of the urgency of this task. First, the physical enormity of the topic and related challenges are worth mentioning. The world's internet architecture and, by extension, our domestic infrastructure is highly integrated with varying levels of resiliency and redundancy. In some cases, there are international norms, although laws and policies often vary by country and by sector. There are many points of failure in this physical internet, and it remains so contested and complex that even risk managers lack full awareness on how to identify and mitigate threats or weaknesses.

Second, our own intelligence community provides sobering assessments on adversarial use and exploitation of the internet. The DNI [Director of National Intelligence], in the most recent Worldwide Threat Assessment, has noted that, quote, "Our adversaries and strategic competitors will increasingly use cyber capabilities, including cyber espionage, attack, and influence, to seek political, economic, and military advantage over the United States and its allies and partners," end quote.

And the physical internet architecture we will talk about today is the highway upon which these adversaries travel. So what is crystal clear, going into today's hearing, is that our adversaries understand our vulnerabilities and will not hesitate to exploit these weaknesses to further their strategic and economic objectives.

We are no longer peerless and security is not assured. In fact, we see these same adversaries, most notably China and Russia, adapting to and learning from our own weaknesses by building what amounts to their own state-controlled internet architecture to monitor, control, and influence their own populations. These very same controls will make it harder for us to preserve and protect geopolitical, offensive, and strategic options for our Nation and our economy.

As I have said many times before, cyber threats from state and non-state adversaries are real, pervasive, and growing. They leverage and integrate cyber information and communications technologies for geopolitical and economic gain in a seamless way. Yet while these adversaries continue to use the internet as a means to achieve strategic objectives, I remain concerned that we as a Nation do not yet have a holistic strategy in place to mitigate, deter, or oppose their advances. This is particularly true regarding the security of our physical internet architecture, the topic for today's timely hearing.

Although not the lead agency on this topic, I am pleased that the Department of Defense is represented at the table today, since they play such an important role in this area, not the least of which may be providing expertise to other agencies during sensitive national emergencies.

We all know that DOD research played a central role in the development of today's internet through the creation of ARPANET [Advanced Research Projects Agency Network]. And today, the Defense Advanced Research Projects Agency, or DARPA, continues to advance our national security through projects related to the resiliency of our Nation's internet architecture, and various other sectors, such as the electrical grid, through their Information Innovation Office.

In the oversight we have conducted on the Armed Services Committee, I feel confident saying that we have improved our military cyberspace and information warfare capabilities, and also improved our resilience in many areas. And while a great deal of broader interagency cooperation and coordination has taken place over the past few years, much work remains to secure our Nation's internet architecture and related sectors, to ensure we remain fast, agile, and resilient even during times of crisis.

And although today's panel is comprised of government experts, we should not forget about the important role that the private sector and defense innovation and industrial bases play, so that we develop a truly whole-of-nation strategy to understand and mitigate these vulnerabilities. Only then will our Nation be prepared for the 21st century challenges we face.

Our witnesses, again, are very well-qualified to help us navigate these multidimensional problems, and I thank them for being here today.

Thank you, again, to the chairman. And, with that, I yield back.

Mr. LANGEVIN. I thank the ranking member.

And now, I would like to recognize and turn to my partner, my colleague, the chairman of the Government Oversight and Reform's Subcommittee on National Security, Mr. Lynch.

STATEMENT OF HON. STEPHEN F. LYNCH, A REPRESENTATIVE FROM MASSACHUSETTS, CHAIRMAN, SUBCOMMITTEE ON NATIONAL SECURITY, COMMITTEE ON OVERSIGHT AND REFORM

Mr. LYNCH. Thank you very much, Mr. Chairman.

Good afternoon to our distinguished panel of witnesses. Thank you for your willingness to help the subcommittees with our work.

Before I begin, I would like to first personally thank my good friend Chairman Jim Langevin and his staff, as well as Ranking Members Stefanik and Hice and their staff, for their cooperation and willingness to collaborate with us on this very important hearing.

Mr. Langevin, in particular, has been a strong and longtime advocate for improving the infrastructure of our country in this measure, and ensuring that necessary cybersecurity safeguards are in place to protect the United States against the multitude of threats that we face each and every day. He has made this issue a priority and it is one that I share, as chairman of the House Oversight Subcommittee on National Security.

Today's hearing will examine how Federal departments and agencies work together to protect the critical architecture upon which U.S. internet and telecommunications systems depend. By working together on the issue, we hope that our subcommittees will better understand and be better positioned to identify and fill gaps and vulnerabilities across the various Federal agencies and private sector for the purpose of protecting our Nation's internet infrastructure.

Uninterrupted and secure access to the internet is critical to daily life in the 21st century. Our constituents rely on the internet to search for jobs, access bank accounts, read the news, and communicate with family. Companies in every industry, from Midwest manufacturers to the financial sector in New York, need the internet to participate in the national and international economy. The U.S. military requires reliable and secure access to the internet to conduct overseas operation, and it is also tasked with protecting our networks from cyber intrusions by foreign actors.

Improving secure and reliable access to the internet is also vital to economic development and promoting livelihoods in less-developed countries or areas. In fact, our committee, I just came back from last weekend, in a congressional delegation to Jakarta, where I met with young entrepreneurs from the Indonesian financial technology sector, who all highlighted the need and importance of expanding internet connectivity across Indonesia, more than 7,000 islands, to bring additional customers into the digital financial market, and to bank the unbanked.

Given our growing dependence on the internet, even temporary disruptions, regardless of whether they are intentional or accidental, can have serious and cascading effects across industries and among our Nation's critical infrastructure sectors. Yet no single U.S. Government entity is responsible for securing the internet and its underlying architecture. Instead, we have multiple departments and agencies, which have various jurisdictional roles, including the Department of Homeland Security, the Department of Defense, the Department of Commerce, from which we are fortunate to have representatives before us today, in addition to the White House, the Department of Energy, the Department of Justice, the Federal Communications Commission, which all have a role to play in securing this infrastructure.

Adding to the complexity of this task is the fact that the physical components of our Nation's telecommunications infrastructure, such as fiberoptic cables and data centers and internet exchange points, are largely owned by the private sector. This means that coordination and communication within the Federal Government, and across the public and private sectors, are all crucial to the internet security.

The challenge we therefore face is that when everyone is in charge, then nobody is in charge. And while internet activity appears to move seamlessly across digital pathways, this movement is cemented in real physical architecture and infrastructure. The security, which has often been taken for granted, in physical fiber cables buried under our streets and under international waters, carries this traffic from point A to point B. Data centers and internet exchange points serve to store and transfer this traffic from network to network.

All of these physical assets can be damaged by natural disasters, human-caused accidents, or intentional attacks by sophisticated malign actors. As Ranking Member Stefanik has noted and as former Director of National Intelligence Dan Coats highlighted in his 2019 Worldwide Threat Assessment, we know that our adversaries are already probing U.S. electric utility grids, election systems, pipelines, and financial networks for any signs of weakness. China, Russia, Iran, and North Korea are all increasingly using cyber operations to steal data, disseminate misinformation, and I quote, "to disrupt critical infrastructure," close quote.

Russia, Director Coats said, and I quote, "is mapping out critical infrastructure with the long-term goal of being able to cause substantial damage," close quote. Multiple open source reports in recent years have also noted increased foreign military activity around undersea data cables, raising concerns that hostile actors could be looking for ways to interfere with this critical infrastructure.

To our witnesses, I realize that some of today's questions may drift into topics not suitable for an unclassified hearing. With that in mind, I just ask that you do your best to answer members' questions as candidly as possible, but you should not disclose any classified or sensitive security information. Instead, please let us know that you would prefer not to respond for national security reasons in an unclassified setting, and we can move on to the next question. We will, however, reserve the right to request that that information be disclosed in a more appropriate setting at a later date.

So, Mr. Chairman, I want to thank you, again, for your courtesy in holding this important hearing with me, and with that, I yield back.

Mr. LANGEVIN. Thank you, Chairman Lynch. And I appreciate your dedication to national security issues. It has been great partnering with you on this topic and look forward to others as well.

With that, I would like to recognize Ranking Member Hice for comments.

STATEMENT OF HON. JODY B. HICE, A REPRESENTATIVE FROM GEORGIA, RANKING MEMBER, SUBCOMMITTEE ON NATIONAL SECURITY, COMMITTEE ON OVERSIGHT AND REFORM

Mr. HICE. Thank you very much, Mr. Chairman, and I would like to thank you and Ranking Member Stefanik for hosting this. And always an honor to work with Chairman Lynch. We appreciate you having us here today, as members of the Subcommittee on National Security as part of the Committee on Oversight and Reform. We appreciate you having us here, and for having this important hearing.

You know, I sometimes have been, with this hearing, somewhat struck by the reactions of different people to this topic. Some may look at this as not among the most flashy topics, but it has got to be among the most important. And more and more, whether we realize it or not, our lives are happening on the internet. Whether it be in commerce or energy or health care or national security, our lives are impacted greatly by the topic and the discussion today. And that is why it is imperative for us to be able to come together and to have a heart-to-heart, honest, open discussion as to what is involved in keeping our Nation's infrastructure safe and secure.

And so I want to sincerely say thank you to each of our witnesses for your role and for you being a part of this hearing today, and I look forward to hearing how you are engaging the various stakeholders, whether they be in government or in the private sector. I want to personally better understand how we are taking a whole-of-government approach to this issue, and if we are not, then I want us to talk about how we get there.

I am also curious to know how each of your components are working together. And there are a lot of seats, if you will, at the internet architecture table, if we can put it that way. And if there are too many seats, we need to know about that; if there need to be fewer seats, we need to know about that.

The internet, for a lot of people, is an unknown territory, but for those of us here in Congress, this is certainly an area that we need to dig deeper into, and make sure that we are secure. And, you know, this is not something that we can say this is in the future. This is where we are currently living. And so, we have got to address this straight up. And so, I deeply thank you for being here. I look forward to our discussion today.

And, again, many thanks to you, Mr. Chairman. And with that, I yield back.

Mr. LANGEVIN. Thank you, Ranking Member Hice.

With that, the chair now recognizes Ms. Manfra, Director Manfra, for her opening statement for 5 minutes. Ms. Manfra, the floor is yours.

STATEMENT OF JEANETTE MANFRA, ASSISTANT DIRECTOR FOR CYBERSECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. MANFRA. Thank you, sir. Chairman Langevin, Chairman Lynch, Ranking Member Stefanik, Ranking Member Hice, and members of the subcommittees, thank you for today's opportunity to discuss this very important issue around securing our Nation's internet architecture, and, specifically, our role, the Cybersecurity and Infrastructure Security Agency, or CISA, role in securing that.

Safeguarding and securing cyberspace has long been a core Homeland Security mission. In today's globally interconnected world, our critical infrastructure and American way of life face a wide array of serious risks. Nation-state adversaries and competitors seek to advance their objectives through various hybrid tactics, including subtle actions that significantly weaken the foundations of U.S. power, degrade society's functions, and increase adversaries' ability to hold our critical infrastructure at risk.

As network devices further weave into our lives and businesses, their vulnerabilities provide additional attack vectors. Global supply chains introduce risks of malicious activity in software and hardware. Many of these risks are complex and dispersed geographically and across stakeholders.

To meet this urgent national security need, Congress established CISA last year. CISA is the Nation's risk adviser, and we are uniquely positioned to serve this role. By statute, and at the President's direction, we lead the Nation's risk management efforts by bringing together diverse stakeholders to collaboratively identify risks, prioritize them, develop solutions, and drive those solutions, to ensure the stability of our most crucial systems.

An important note is that we don't just think about threat or vulnerability or consequence; we think about them all together and how they interact in order to establish risk. And so, we try to understand things, how could an adversary actually accomplish something, can they have an actual consequence. So when I talk about risk management, that is how we frame it.

So, as the Nation's risk adviser, we must also unify two strategic goals across all of our mission space. We must simultaneously mobilize strong public-private partnerships to defend against the most urgent threats and hazards, while not losing sight of the need to build a more secure tomorrow. Our foremost responsibility is to safeguard the American people, and we prioritize our efforts at all levels to focus on the greatest risks facing the homeland. In order to successfully accomplish this, we must be able to understand and manage this risk holistically. And, again, that means we must understand both threat and vulnerability and the consequence, and we must also understand how that manifests across the country.

This is why we established the National Risk Management Center. CISA, while often referred to as a cyber agency, is more than just cyber. In fact, we have a long history in thinking about infrastructure security holistically, both against natural and man-made hazards. By establishing the National Risk Management Center within CISA, this brings together all our different disciplines to better understand what is the risk to the Nation as a whole.

Our first important step was to reframe the conversation. Instead of thinking about industry-specific activities, but to think about cross-cutting functions, because in the end, adversaries are interested in causing consequences to the functioning of our society, or holding those at risk. Therefore, we worked across multiple sectors of the economy and government partners to establish the first set of national critical functions in early April of this year. These national critical functions support the operations of nearly all businesses, public safety organizations, and government, and are so vital that their disruption, corruption, or dysfunction would have a debilitating effect on our Nation.

The global internet architecture includes an array of components that enable these national critical functions. Going forward, we will prioritize our efforts and resources, both within CISA and across the government, to ensure we are reducing risk to these functions and bringing the full power of the U.S. Government to bear to do so.

At CISA, our vision is to fully realize this national effort that I just described. This means breaking down the old organizational and institutional divides that impede our ability to provide for our collective defense in cyberspace. Our adversaries are targeting systems that are across sector, and the growing interdependencies demand an integrated approach. To achieve this integrated approach, we are working and we will continue to work with numerous stakeholders, including my colleagues joining me today.

Specifically, we have been working with the National Telecommunications and Information Administration, or NTIA, for many years on multiple internet governance issues from Domain Name System, or DNS, issues to participating in our multi-stakeholder process to publish a report on botnets.

We also have expanded our partnership with DOD. Almost a year ago, DHS and DOD finalized an agreement which reflects the commitment of both departments to this important issue. This agreement clarifies roles and responsibilities to enhance U.S. Government readiness to respond to cyber threats, and establishes coordinated lines of efforts to secure, protect, and defend the homeland.

Today's national security challenges require innovation in government as well as in the economy and throughout the world, and I am proud to be working with two partners who share that desire for innovation and partnership.

The heart of CISA's purpose is to mobilize a collective defense of our Nation's critical infrastructure, and we cannot do this alone. My colleagues on this panel represent some of those critical partnerships in order to achieve this goal.

Tomorrow is the anniversary of the September 11th attacks on our country. As we learned from that event 18 years ago, information and Federal operations must not be siloed. We see these same lessons amplified and complicated by the global, borderless, interconnected nature of cyberspace, where strategic threats can manifest in the homeland without advance warning.

I thank you again for starting this important conversation and holding this hearing, and I look forward to further discussing our efforts. Thank you, and I look forward to your questions.

[The prepared statement of Ms. Manfra can be found in the Appendix on page 46.]

Mr. LANGEVIN. Thank you, Director Manfra.

Administrator Rinaldo, you are recognized next.

STATEMENT OF DIANE RINALDO, ACTING ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION, AND ADMINISTRATOR, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Ms. RINALDO. Chairman Langevin, Chairman Lynch, Ranking Member Stefanik, Ranking Member Hice, and members of the committee, thank you for the opportunity to testify today on the role of the U.S. Government in securing the Nation's internet architecture.

The National Telecommunications and Information Administration in the Department of Commerce is responsible for advising the President on telecommunications and information. NTIA collaborates with other Commerce bureaus and executive branch agencies to advocate for domestic and international policies that preserve the open internet and advance the key U.S. interests.

NTIA is involved in a host of policy issues that affect the security of critical elements of our Nation's telecommunications infrastructure. Our support includes working with our interagency partners to enhance the security of our Nation's telecommunications supply chain. We are supporting the Secretary of Commerce on the implementation of the Executive order on securing the information and communications technology and services supply chain.

NTIA is the lead executive branch expert agency on issues relating to the Domain Name System, a critical component of the internet architecture. The DNS functions similar to an address book for the internet by allowing users to identify websites, mail servers, and other internet destination using easy-to-understand names.

NTIA supports a multi-stakeholder approach to the coordination of the DNS to ensure long-term viability of the internet. NTIA collaborates across the government on numerous efforts related to the security of the Nation's internet architecture.

We have been working closely with the National Security Council and the interagency colleagues on implementing the National Cyber Strategy. In that effort, we share our activities across the interagency and look for synergies to maximize the impact of the strategy. NTIA will continue to participate in these efforts.

One significant example of NTIA's contribution to the protection of the internet infrastructure is our work with NIST [National Institute of Standards and Technology] and DHS on the Botnet Report, delivered to the President in May of 2018. Botnet attacks can have large and damaging effects, and they put the broader network at risk.

Botnets now capitalize on the sheer number of Internet of Things connections and devices. We have seen attacks that have topped a terabyte per second. Dealing with an attack of this magnitude can take time, which is a major concern when dealing with critical infrastructure.

The Botnet Report outlines a positive vision for the future, cemented by six principal themes and five complementary goals that would improve the resilience of the internet ecosystem. The Departments of Commerce and Homeland Security developed the report through an open and transparent process for the specific purpose of identifying stakeholder actions as opposed to government regulation.

We are tracking progress through a document known as the Botnet Road Map. More than half of the identified tasks are already in progress or completed. At the end of this year, the Departments of Commerce and Homeland will provide a status update to the President that reviews progress, tracks the impact of the road map, and sets further priorities.

NTIA's cybersecurity multi-stakeholder processes also contribute to the security of the Nation's internet architecture. Most recently, we have been working on a software component bill of materials. Most modern software is not written completely from scratch, but includes existing components from the open source and commercial software world, which can be challenging to track. Our ultimate objective is to foster a more resilient ecosystem through industry-led, market-based cybersecurity solutions.

Over the past three decades, the internet has been transformational for the American economy. America's established leadership in technology has resulted in millions of jobs and remarkable prosperity. Because of this, we must work harder than ever to ensure that the infrastructure supporting the internet is secure. NTIA is committed to coordinating across the Federal Government and engaging with the private sector to ensure the United States can continue to harness the economic benefits of this vital part of the economy for American businesses and for American workers.

Thank you for this opportunity to testify, and I look forward to your questions.

[The prepared statement of Ms. Rinaldo can be found in the Appendix on page 54.]

Mr. LANGEVIN. Thank you, Ms. Rinaldo.

Mr. Wilson, you are now recognized for 5 minutes.

STATEMENT OF B. EDWIN WILSON, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY, OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR POLICY, U.S. DEPARTMENT OF DEFENSE

Mr. WILSON. Chairman Langevin, Chairwoman Stefanik, Ranking Member Hice, and Ranking Member Stefanik, my apologies, Chairman Lynch, and the members of the subcommittee, thank you for the opportunity to testify before you today.

Mr. LANGEVIN. Can you pull the mic a little closer to you, General?

Mr. WILSON. Absolutely. Is that better, sir?

Mr. LYNCH. You might want to turn it on.

Mr. LANGEVIN. Is it on?

Mr. WILSON. I have got a green light. My apologies.

Chairman Langevin, Chairman Lynch, Ranking Member Stefanik, Ranking Member Hice, it is really an honor to be here before you and the subcommittee members. It is good to be back in this Chamber, as well, testifying again. I look forward to discussing the role of the U.S. Government in securing the Nation's internet architecture alongside my counterparts from the Department of Homeland Security and Department of Commerce. It is a critically important topic. We understand the sense of urgency behind this.

First, on behalf of Secretary Esper, thank you for the tremendous support that Congress has given the Department of Defense in our effort to improve our overall defense posture related to cyber threats. We have made significant progress, but with your support we continue to make significant progress to deter, disrupt, and defeat strategic malicious cyber threats directed at our national interests. Despite this progress, we understand there is much more that needs to be done. And, with that, we have been very, very focused on the progress ahead.

As the 2018 National Defense Strategy and the 2018 DOD Cyber Strategy make clear, the U.S. homeland is no longer a sanctuary from cyber threats. Our strategic competitors, such as China and Russia, are conducting persistent cyber-enabled campaigns to erode U.S. military advantage, threaten our Nation's critical infrastructure, and reduce our economic prosperity, which includes threats to our telecommunications and information technology sectors.

These campaigns are being conducted below the threshold of armed conflict, but collectively pose long-term strategic risk to the Nation, our allies, and our partners. In response, the Department adopted a proactive posture to compete with and counter determined and rapidly maturing cyber adversaries. Our objective is to prevent or mitigate significant threats before they reach U.S. soil. We refer to this strategy as defending forward. It is the core of our DOD Cyber Strategy.

This approach is focused on enabling our interagency, industry, and international partners to strengthen their resilience, close vulnerabilities, and defend critical networks and systems, while simultaneously imposing costs on adversary malicious cyber actors when called upon. Towards this end, the Department is continually working with our partners, both domestically and internationally, to strengthen the resilience of networks and systems that contribute to current and future military advantages.

The Department previously focused its defensive efforts almost exclusively on military platforms, systems, and networks. However, the evolving cyber threat [and] increasingly proactive activities of key competitors have demonstrated vulnerabilities that extend beyond our DOD systems and networks. The vulnerability of critical infrastructure to cyberattacks means that adversaries could disrupt military command and control, banking and financial operations, the transportation sector, the energy sector, various means of communication, and a variety of other sectors. As a result, supporting U.S. Government efforts in securing and defending the Nation's critical infrastructure is a key priority under our DOD Cyber Strategy.

Partnerships are an essential element of our National Defense Strategy. We understand that our interagency, international, and industry partners are vital to ensuring that DOD can operate and project power in a contested cyber environment. DOD's role in defending the homeland is outwardly focused, like it is in any other domain of operations, focused on strategic threats and supports our interagency partners, including the Department of Homeland Security and the other sector-specific agencies.

The U.S. Government has a limited and specific role to play in defending against attacks on our Nation's internet architecture, including through our trusted relationships with industry. As we all recognize, security was not a primary consideration when the internet was designed and fielded. Although computers and network technologies underpin U.S. military warfighting superiority by enabling the joint force to gain the information advantage, strike at long distances, and exercise global command and control, the private sector was and operates now well over 90 percent of the interdependent networks of information technology infrastructure across the cyberspace domain. At the same time, the Nation's telecommunications infrastructure is primarily owned by commercial entities.

Our adversaries target our Nation's weakest links, and vulnerabilities are consistently found across the full scope of the internet ecosystem, be it government or industry.

The Department, which views the challenges it faces in performance of its critical missions principally through a national security lens, is nonetheless highly dependent on privately owned infrastructure, decisions concerning which are regularly guided by ordinary business or economic considerations. Recognizing this inherent tension, defending national critical infrastructure, including the Nation's internet architecture, from significant foreign malicious cyber activity has become an area of interest and emphasis for the Department.

A large-scale disruption or degradation of national critical infrastructure would constitute a national security concern, as would threats to the DOD critical technology information, other controlled unclassified information, processes stored on non-DOD-owned systems and networks, which demands a close cooperation alongside our partners.

This reinvigorated partnership alongside the FBI [Federal Bureau of Investigation], intelligence community, was instrumental to the whole-of-government efforts to protect and defend the 2018 U.S. midterm elections from foreign interference. We continue to leverage the lessons from this experience and these activities to help shape and further improve how we secure 2020 elections and other ongoing efforts related to protecting and defending the Nation's critical infrastructure.

Again, thank you for the opportunity to appear before you today and for the continued support you and your staffs provide as we address these challenges. I look forward to your questions.

[The prepared statement of Mr. Wilson can be found in the Appendix on page 61.]

Mr. LANGEVIN. Thank you, Mr. Wilson.

We are going to go and do questions at this point. Members are recognized for 5 minutes. Before we go to that, though, I just want to mention that we are expecting votes in just a few minutes, so we will get through as many of the questions as possible. So if we can all stick to as close to 5 minutes in questions and answers, that will move things along.

So, with that, I want to begin for all of our witnesses the question: What role does the National Security Council and the White House play in facilitating and coordinating amongst all the Federal agencies, and can you describe efforts led by the White House to address internet architecture security? Ms. Manfra, if we could start with you.

Ms. MANFRA. Thank you for the question, sir. Well, the National Security Council, as a policy coordination body, focuses on, from the cyber perspective, but also on the resilience side, areas that we need to either identify or implement policies as an interagency body.

They coordinated the National Cyber Strategy, which was released some time ago. And in focusing specifically on, as an example, things like the DNS ecosystem, supply chain for our ICT [information and communication technologies] ecosystem, and as well as other threats that may come up, coordinating both the policy and any kind of response that we may need to do, either urgently or in the long term.

Mr. LANGEVIN. Ms. Rinaldo or Mr. Wilson, can you comment on any aspects of interactions with the White House on coordination?

Ms. RINALDO. Yes. As Ms. Manfra said, the White House routinely convenes meetings to bring us together to talk about issues as the cyber strategy, supply chain, as well as other issues that come up, as needed. It is an opportunity to bring not only my two fellow witnesses to the table, as well as other parts of the government that may have equities in these processes as well.

So they are fairly routine, and with the cyber strategy we have due out, so we regularly meet to see where we are on the process of implementing that.

Mr. LANGEVIN. Thank you.

Mr. Wilson.

Mr. WILSON. And I would just add, in the series of sessions that we do do across the interagency led by the NSC [National Security Council] team——

Mr. LANGEVIN. Can you pull that microphone a little closer?

Mr. WILSON. Can do. I am going to put on my command voice and project, if that is okay then. My apologies.

As we do, we look at a lot at the threat, we bring in especially the intelligence community to understand the threat, as well as a series of functional reviews that we do with recommendations that follow. And that could be the report that was referenced earlier about the botnet. It could be work that is going on regarding ransomware across the interagency.

Sometimes it will start domestically, but then we will bring in a larger team if we see some initial work at the direction of the NSC team. And so, depending on the topic, there is usually a series, but many times, we are organized to be able to address specific threats and understand that threat so that we have the right actions.

Mr. LANGEVIN. Ms. Manfra, what is the role of law enforcement agencies, such as the FBI and CISA's own Federal Protective Service [FPS], in protective or defensive functions such as hardening cable landing stations and IXPs that are owned and operated by the private sector?

Ms. MANFRA. Sir, we have a very close partnership with the FBI in particular, specifically on some of these issues. The FBI is able to kind of cross both on the intelligence side as well as law enforcement authority, both to take actions, you know, legal actions, if needed, through the justice process against those who may not be following legal laws related to how they are deploying their systems as well as conducting investigations that we may be gathering from intelligence sources, so working domestically to further investigation to determine is there an issue.

Other law enforcement entities are not as involved on the internet architecture issue itself, though they have the ability to collect information, or if they have a related case, to share that information.

FPS is primarily focused on physical protection of government buildings, and we have worked with them on ensuring that building owners are thinking holistically about cyber and physical threats to their buildings, but not particularly relevant, probably, to the internet architecture conversation.

Mr. LANGEVIN. I think that is—again, the whole purpose of this hearing is so we get a better understanding of what we need to continue to focus on, in terms of hardening these sites.

Let me just——

Mr. WILSON. Chairman Langevin, if I could maybe just add on, the DOD has a very active role alongside DHS as well, both domestically and internationally. And so we work with industry partners, but domestically, especially with DHS, to understand what information flows are moving through, so from a command and control perspective or communications flow to our forces to do assessments, and to understand that we have enough capacity and diversity of undersea cable, you know, capability to be able to execute our DOD missions.

To go into more detail, I probably need to go into a classified session, but just to make you aware that we have a very active relationship alongside our interagency partners, very tied to our mission and execution of the DOD missions around the world. So it is more of an international perspective.

Mr. LANGEVIN. Thank you.

I believe my time is expired, so I am going to stop there. We are going to have some follow-up questions I would like to submit for the record, and I ask you to respond to those. And, with that, I believe votes have been called.

I am going to yield to Ranking Member Stefanik and, hopefully, we can get through her questions.

Ms. STEFANIK. Great.

Given the complexities of the ecosystem that we are talking about today, I want to focus on supply chain security and integrity, which many of you referenced in your opening statement. I would like to understand in more detail, given how complex the global telecommunications supply chain already is, combined with emerging technologies like 5G, Internet of Things, even cloud computing, how are you specifically improving our supply chain security? Ms. Rinaldo, I will start with you. That is question one.

The second one is, are there any specific technologies you are more concerned about than others in securing our supply chain; and specifically, what collaboration needs to happen with industry and the private sector? So, Ms. Rinaldo, I will start with you.

Ms. RINALDO. Great, thank you. As you may know, on May 15th of this year, the President issued Executive Order 13873, securing the information and communications technology and services supply chain, which gives the Secretary of Commerce IEEPA [International Emergency Economic Powers Act] authority, emergency powers to act on national security concerns with the implementation of infrastructure into our telecommunications networks.

This is something that NTIA is working with the Secretary's office on. We are currently developing the interim-final rule of the regulations on how this process will work out. We believe that we are on track to have that delivered to the President the middle of October.

But as well, through our multi-stakeholder processes, which we are probably most known for, is an opportunity for us to meet with technologists, policy makers, academia, civil society to talk about these important issues. The thing that I really love about NTIA is that we are able to pull back to the 50,000-foot level and look, and then hone in on certain issues and go down and tackle certain concerns or issues. And this is the format that we use.

So we talk about vulnerabilities. We are currently working on the software bill of materials specific to supply chain. We definitely have concerns moving forward, especially as we move to fifth-generation technologies. And I think it really gives us an opportunity, as we talked about, is it, you know, baked in or bolted on, that it gives us the opportunity to bake in security as we move forward.

Ms. STEFANIK. Ms. Manfra.

Ms. MANFRA. Yes, ma'am. I will just touch high level, and then we can—always happy to come back and go in more depth. There is a lot to talk about on supply chain.

As Diane noted, around the Executive order, that is a key component of the administration's approach, we at CISA have also stood up an ICT Supply Chain Task Force, which is mostly made up of private sector, but also colleagues across the government, to focus on what are the most important things that we can actually make progress on, what are the tangible things we can do. And they have been working along a few of those lines, particularly around procurement, government procurement, which, to segue into what we are doing for government procurement, following up on the law that was passed last December around Federal acquisition security and supply chain chaired by Grant [Schneider], but an interagency body to look at how do we reform and modernize our Federal procurement system to ensure that we are taking mission risk, I will call it, into account when we are procuring and maintaining IT [information technology] products and services.

So those are some of the things that we are doing. Specific technology, I would say it is not necessarily a specific type of technology that is concerning. What we have, really, from a DHS perspective is we really think of it as a framework that started with our experience in Kaspersky, but that you have to really look at where is this product or data being held, what are the laws of the country that mandate how that data or products are treated, but you also have to look at what is the level of access that that piece of software, or that piece of hardware, that somebody would be able to gain access to. And at various pieces of software, you have tremendous access into a computer.

So that, combined with a country's laws that we have concern about that would compel access, those things together are what would cause us concern. So we are looking at a lot of things and across the government is how do we understand things like foreign ownership and controlling influence? How do we understand what that means to risk? But looking at it through that framework. And then, of course, what would always be the consequence, that somebody who had that access and those laws, is there any sort of significant consequence? So it is less about the technology and more about the context that that technology lives.

Ms. STEFANIK. My time is expired. Mr. Wilson, I will take yours for the record since we have expired.

I yield back.

[The information referred to was not available at the time of printing.]

Mr. LANGEVIN. I thank the ranking member. So votes have been called. We are going to recess at this point. We will return right after. There are three votes, so hopefully we will get through those quickly and we will come right back, and then Chairman Lynch will be up next for questions.

The committee stands in recess.

[Recess.]

Mr. LANGEVIN. The subcommittee will come to order. I will next recognize the chairman of the Oversight and Reform Committee, National Security, Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Chairman. Again, I really appreciate your willingness to come here and help us grapple with these problems. Recently, I have had groups ask to meet with me about the need for more funding from the government for infrastructure security. And when you sort of look at the landscape here, you know, you have Facebook and Apple and Google and other private sector players that have a major role here, and that have an intense investment, I think, in maintaining security themselves.

Do you think there is a significant role here to play in funding the necessary improvements to our infrastructure on the part of, you know, internet companies, including mobile banking and others, much the same way that, you know, we have a gas tax for the users of our roads and highways that goes into the transportation trust fund and helps with an enormous part of the funding for that infrastructure?

Have you thought about this from a funding side in terms of how we have to continually maintain the integrity of the internet architecture, and in a way of doing that over the long term? So I would offer it to the three of you, if you have thought about this aspect of it. Ms. Manfra.

Ms. MANFRA. Yes, sir, I can start. Yes, the funding question is something we grapple with in a lot of areas. I will say, when you are talking about those companies that provide the internet architecture, the ecosystem that we are talking about, as you noted, they have a lot of economic incentives to have a secure and reliable infrastructure. So I don't know that we have considered sort of funding those organizations. They are also doing very well, as I understand it, and have a fair amount of funding. There are other elements when you get into State and local organizations and others that I think is a separate conversation.

I will say when we think about how the government could provide resources in this space in either complementing private sector investment or driving change, it would be in the area of standards and research and development. In how do we think about—what sort of—there are some standards bodies, there could potentially be new standards bodies, or existing ones that evolve, to think about things like 5G, and as our, kind of, overall internet architecture evolves, the government thinking about how do we participate in that process either through resourcing or participation.

And, importantly, I think in research and development, how do we think of new ways to build more resilient infrastructure, both resilient from a physical perspective and a cyber. So those would be the areas that we have most thought about the funding.

Mr. LYNCH. Thank you. Ms. Rinaldo.

Ms. RINALDO. When you look at the ecosystem as a whole, most private companies underpin the internet architecture. So what added benefit can government bring them to help move the ball? At NTIA, we currently work with the private sector through our webinars. We have a broadband group that actually reaches out to rural areas to talk to local providers on how can we help them improve their security and their resiliency.

We work through the American Broadband Initiative, which the President initiated last year. We lead that on behalf of the government, to, again, have these conversations on how can we as a government help improve security and resiliency? And one of the things that we hear back is information sharing, something as—Chairman Langevin, we talked about just before the hearing that I have been working on for a very long time. What information can we pass as a government to local providers, to vendor manufacturers, to ensure that they are getting the quality of information to help them protect their products that are being implemented throughout the supply chain?

Mr. LYNCH. Thank you. Mr. Wilson.

Mr. WILSON. I would just echo. I think when we look from a DOD perspective, we look for the nexus when it revolves around national security. And so, we are very active in standards boards, not just domestically, but globally, associated with the internet. In addition, we look at capability that could be brought to bear from a DOD perspective.

We are very active in the research and development, it was highlighted in the introductory comments, the defense—the DARPA team. Also, our service laboratories, and I would also have to tip my hat to the Department of Energy lab environment. They do some great work in this arena. There is a lot of partnering that goes on to bring innovation to the game—to this table in terms of solutions. To be really a catalyst for change. And there is several different——

Mr. LYNCH. What about cost sharing, that is what I am asking. From the private sector, you know, they are the major beneficiaries, these private companies that are, you know, hugely successful.

Mr. WILSON. Uh-huh. So in the Department of Defense, we use a vehicle such as cooperative research and development agreements with industry partners, really a sharing of either personnel in intellectual property as well as resources. So we may have a range in the Department of Defense where we can do, you know, experimentation, et cetera. So we use several different vehicles along those lines to be able to get after high-priority requirements.

Again, we look for the national security nexus when it comes to research and development standards, et cetera.

Mr. LYNCH. Okay. Thank you very much, Mr. Chairman. I yield back.

Mr. LANGEVIN. Thank you very much. And Mr. Hice—Representative Hice is now recognized.

Mr. HICE. Thank you very much, Mr. Chairman. Mr. Wilson, while you were talking, we will just keep going here. About this time last year, the Department of Defense released a cyber strategy where it was highlighted the need to conduct cyberspace operations. It is very intriguing to me, and specifically to determine and to make sure that we are able to maintain our U.S. military advantage, and at the same time, to defend our national interest.

And in an interesting quote, and also, quote: To prepare military and cyber capabilities to be used in the event of a crisis or conflict. Those three areas are extremely important to me, and I know in my own district, Fort Gordon, the Cyber Center of Excellence resides there and they are very much involved in all three of these areas.

Obviously, without going into classified information, but would you be able to share some of the specific actions that the Department has taken in light of that cyber strategy to—just some insight on how things are going to protect our infrastructure?

Mr. WILSON. Absolutely. So in August of last year, the Secretary signed, Secretary Mattis at the time, signed out the DOD Cyber Strategy. Some very core missions. Number one being the ability to operate DOD joint force. So kinetic forces alongside all the other forces in a cyber contested environment, to be able to build resiliency into our joint force. That was priority one from Secretary Mattis' perspective.

In addition, we wanted to be able to bring cyber effects operations, defensive and offensive, alongside our normal kinetic operations. And so, we have been hard at work at doing that. We have worked with Congress, with authorities, to be able to execute in that arena. We usually are pretty—we do some really good work in the area of hostilities in competition with the revisionist powers we have seen, that they are operating below our normal traditional response mechanisms. And so, we have been very focused on that, so the strategy addresses that.

Down at Fort Gordon, they are doing some great work, Lieutenant General Fogarty and team, in terms of—that is the ARCYBER, the Army Cyber team. They are focused right now in CENTCOM [U.S. Central Command] theater, AFRICOM theater, the Africa Command, doing some fantastic work.

When it comes to critical infrastructure, there was a recognition that the Department of Defense had a role. And I think if you had asked us maybe 2 or 3 years ago, it wasn't as clear. We brought a strategy forward called the "defend forward." We focus in the Department, just like we do in any other domain of operations, on external threats to the Nation, and so in cyberspace we do the same things. We focus on those external threats. We want to be able to see those threats, understand those threats, see indications and warnings if there is attack on critical infrastructure for the Nation, or DOD forces or allies. And we want to be postured and prepared to be able to respond to those attacks; preferably in a preemptive fashion, if needed, versus waiting to take a strike and then have to be——

Mr. HICE. Would you believe—how are we doing is kind of what I want to know. Are we prepared offensively? Are we prepared defensively? Are we prepared in the event of a crisis here? I mean, where are we on these three areas? On a scale of 1 to 10, I mean, are we——

Mr. WILSON. So it depends on which category, and it is best done in a classified setting, but maybe I can put a backdrop behind it. We are making tremendous progress. Over the last year, we have executed operations which we have briefed in the Armed Services updates, and we are getting ready to do one here shortly, across different—several different mission types. And so, that is going very well on the offensive side.

On the defensive side, we are building tremendous resiliency in the force; we have a long way to go. So, if you are talking about the network, we have tremendous activity going on end point security zero trust environment, and the team is doing really good work. We also have activity going on associated with weapons systems to make them more resilient. And then we are beginning to look at defensive cyber effects operations broadly to be able to mitigate risk to the best of our ability.

Mr. HICE. Okay. Well, Mr. Chairman, I don't have time to get into the next question, so I will go ahead and yield back. Thank you.

Mr. LANGEVIN. Thank you. Mr. Kim, I recognize you for 5 minutes.

Mr. KIM. Thank you, Mr. Chairman. I thank you so much for being here and being able to have an interagency discussion about this. I would like to just hone in on just some of my understandings about some vulnerabilities and try to get a better sense of how different agencies and departments are honed in on this.

A concern that we have is certainly about the different nodes in which the information is coming to us through internet exchange points. We have one in New Jersey and we understand some of the vulnerabilities that come with that. When information is being transmitted through, let's say, the undersea cables, through the internet exchange points, I, from my understanding, is that the undersea cables is something under the jurisdiction of DOD. The internet exchange points are ones under the jurisdiction and oversight of DHS.

So I guess my understanding is how do we structure the preparations or the coordination that is involved in that to try to understand if we were to have any disruptions along those points that we can understand what role different agencies and departments play? Are there particular exercises that are being done? Are there other ways that we can understand who all is engaged, because from what I understand, it's lots of different departments and agencies and offices that are involved in that type of process.

So if you don't mind, I would love to just hear from across the board what we can be doing on that front, and who are the main actors that need to be at that table?

Ms. MANFRA. Thank you for the question, sir. I don't know that I would use the term "jurisdiction." You know, we don't—I wouldn't say we have jurisdiction over internet exchange points, and I would defer to DOD, but I don't think they have jurisdiction over undersea cables. What it is more is, we have some interagency bodies, such as Team Telecom and things like CFIUS [Committee on Foreign Investment in the United States], other sort of bodies where we work together, our three agencies plus others, to understand the risk and make decisions, and are able to intervene, if necessary, in market decisions in those particular cases.

In other areas where there is not a specific investment or acquisition happening, we continue to work together. You know, once you start getting further beyond the borders of U.S. waters, obviously, there are others who start to have insight, but we recognize the connectedness of that. So specifically on undersea cables, we worked with the DNI, 2 years ago, issued a report on threats to undersea cables, working very closely with the DOD, DNI, and others to both better understand the threat, but then on the DHS side, given sort of our authorities and the public private partnerships, what can we do to counter that threat, build more resilience, and, of course, DOD has capabilities to use those tools as well as NTIA.

So it is not so much that here is clear jurisdiction and it ends at this part of the internet architecture, and then the next person picks it up. It is really largely private sector led in all cases, and what we have are different tools to analyze and make assessments and take action if we have some concerns. Is there potential—more tools and better cooperation? Absolutely, we can always continue to improve the coordination, and that is why I think we have got those national critical functions focused on, you know, how is the stability of the internet overall? How are we focusing on that? What are those different mechanisms and those tools and those partners? That is how I would—I hope that is helpful.

Mr. KIM. No, that is helpful. Any of the other witnesses want to jump in on this? Mr. Wilson.

Mr. WILSON. From a DOD perspective, what we really focus and understand, try to understand the threat. So we work with the intelligence community, and then our own insights. Also, we do assessments so that we understand our reliance on cable landing sites or any type of infrastructure. And then we constantly are planning and coming up with contingencies. So based on that reliance, we want to understand if that is lost, in whatever fashion, however complex that looks like, our ability to roll off and conduct operations maybe in a minimized fashion with high-priority taskings. So that is a natural rhythm that we move through in our war plan and OPLAN [operations plan] activities. In addition, in our Tier 1 exercises, we do exercise in the loss of critical infrastructure, which might include cable landing sites or other undersea cables; that is a normal battle rhythm of activity that we look at.

Just, I would point to maybe day-to-day. We do have—there is just, you know, anchor drags and cable losses, and so just naturally, we see in a day-to-day fashion the loss of capability, whether it is natural disasters or man-made calamities out there under the sea, we see that happen on occasion on a very routine basis. And so we are constantly having to already do this for a living, if you will, to maintain mission.

Mr. KIM. Yeah.

Mr. WILSON. So we gain a lot of insight, and we do a lot of afteractions and lessons learned, based on those experiences. And so a pretty deep well of knowledge there and we share and work hand in hand with DHS. We have natural rhythms. They see our tasking orders, we share that from a cyber perspective.

Mr. KIM. Well, thank you for your insights. Mr. Chairman, I yield back.

Mr. LANGEVIN. Thank you, Mr. Kim. Mr. Banks is recognized.

Mr. BANKS. Thank you, Mr. Chairman. I think we all agree as the DOD moves toward an increasingly internet-integrated warfighting posture, it is critically important to identify vulnerabilities in software and hardware within the DOD network.

Mr. Wilson, as identified in DOD's 2019 Digital Modernization Strategy, DOD utilizes 10,000 operational IT systems. I am concerned about the number of access points within the DOD network. Does DOD have a complete inventory of all items that can access the network?

Mr. WILSON. Today, the answer would be we do not. We are driving very, very diligently to have insight and to be able to see. We have several modernization efforts and several initiatives underway, end point security and visibility being the number one. So that we have visibility to all those end points. Ten thousand end points, sir, would probably be a low estimate.

So when you just look at end users out there, given we have several million people inside the Department of Defense, that number is much higher than that. And so, we need to be able to have visibility to be able to mitigate risk. And so step one has been insight, and end point security initiative that has been underway. We are really driving hard. We are getting tremendous traction alongside the services and our Fourth Estate in the DOD enterprise.

In addition, we have an initiative underway called Zero Trust where we are driving, so that we validate and limit the movement so if something is exploited inside the network, that we contain that to the best of our ability. So Admiral Norton and the DISA [Defense Information Systems Agency] team are hard at work on that alongside the service components. And so, it has been a high-priority task. The deputy is taking reviews on all of these initiatives plus more on a very routine basis, so the sense of urgency is high on this one.

Mr. BANKS. Good. Ms. Manfra, you testified that the CISA works across government and industry to ensure the national security and the emergency preparedness community has access to priority telecommunications and restoration. Are government agencies able to keep up with industry in issuing security updates?

Ms. MANFRA. I think much of what we use is industry products. So it is more about ensuring the behavior that people are actually, if you are referring to patching and those sorts of things. We have had a lot of work that we have done around this to focus behavior on those types of things. Are they patching vulnerabilities that are identified? And we have actually made a tremendous amount of progress.

I think we—I think we are able to keep up with them. In some cases, we are actually leading industry. There is work that we have done under one of our directives to improve web and email security, and the government went from least secure by an independent auditor to actually leading all industries in the security of our websites.

So I think that there is—and I think that is what we need to be doing. We should be not just talking about it, but actually leading and putting these things in place. But it is a mix of behavior and resource. Sometimes there is technical challenges and we work with agencies in particular to assist them on that.

But if that is getting at your question.

Mr. BANKS. Yes. Mr. Wilson, back to you. How does the role of the CIO [Chief Information Officer] coordinate with the DISA regarding the responsibility of the DOD IT security?

Mr. WILSON. So the DOD CIO, by statute, has responsibility for the standards and technology and the fielding of capability. DISA is their operations arm. And so, DISA has purview, and there is two roles, organizing, training, and equipping alongside the services, all of our IT fielding.

In addition, the DISA commander, Admiral Norton, also wears what we call the Joint Force Headquarters commander hat for the DODIN, the DOD Information Network. So in that role, she is able to direct activity in terms of orders out to the DOD at large. And so that kind of is the arm that is able to execute operationally day to day to mitigate risk. If there is an incident, to be able to harness the power of the Department at large and be able to mitigate that risk, to be able to drive initiatives like the Zero Trust activity that I just highlighted.

So DOD CIO is responsible statutorily for the Department in terms of standards and compliance. And then the operation arm is DISA that reports up through the DOD CIO.

Mr. BANKS. Okay. Thank you very much. I yield back.

Mr. LANGEVIN. Thank you. Mr. Higgins is now recognized.

Mr. HIGGINS. Thank you, Mr. Chairman. Ladies and gentlemen, thank you for being here this afternoon. I have two questions. One is very basic and the other is rather not. So let's handle the basic question first. How do you ladies and gentlemen feel about securing our undersea submarine cables that transmit most of our signals? How do you feel about that? Where are we right there?

Ms. MANFRA. Well, sir, I would argue that——

Mr. HIGGINS. It has been identified as an area of potential threat.

Ms. MANFRA. Yes.

Mr. HIGGINS. And this could disrupt internet services globally, and have serious economic impact, and perhaps military implications, communications, et cetera. So without getting into the weeds or revealing anything that shouldn't be spoken of, what is your opinion? Is there more that should be done and could be done?

Ms. MANFRA. Yes, sir. This is a high priority for us, both my agency and those here, as well as others that aren't represented, and we are very focused on this. And, yes, there is absolutely more that we will do and can do—is the short answer.

Mr. HIGGINS. You concur, sir?

Mr. WILSON. Yes. For the Department of Defense, it is core to what we do. And so I would just kind of maybe walk back through. One, we want to understand the threat against undersea cables in particular, because we are relying on them. Any time that the DOD is relying on any kind of capability, we want to understand the threat to it, where the vulnerabilities are, and then——

Mr. HIGGINS. Those threats and vulnerabilities, in your opinion, are being addressed?

Mr. WILSON. We understand the threat, and we understand the vulnerabilities. So the next is, how do you mitigate those risks? For us in the military, that would be an operations—the execution of our operations day to day. So we have a very robust effort that we continually look and assess undersea cables, because it is the crux of and we rely on it for lot of our communications——

Mr. HIGGINS. So in the interest of time, and thank you for answering, please, just all of you, stay in very efficient communications with both of these committees, whereby we can give you anything you need because it would be a disaster for the world if those things got hit.

So let's move to my question that is actually my concern. I am concerned about national security issues regarding protection from emerging technologies sponsored by nation-states with global aspirations and strategies like China. Specifically, I am talking about quantum computing. We have a responsibility to protect the people's treasure, and, of course, we have a responsibility to provide national security.

But are we talking about investing money on protecting ones and zeros, long streams of ones and zeros, when China could be on the verge of using entangled photons to communicate. They recently had this public data and satellite transmission to two separate land stations 1,200 miles apart, and achieved quantum entanglement successfully.

A professor from LSU [Louisiana State University] in my home State of Louisiana, a physics professor that spends a large part of the year at the University in Shanghai, the Science and Technology of China university, stated that he believes China will go dark in 2 to 3 years, meaning we won't be able to—we won't be able to understand and read their communications. So if they reach a point through quantum computing before we do, because we are spending money on VHS tapes while the world moved to DVD, if they reach a point of quantum entanglement and quantum computing efficiently and we can't read them, then how would we know that they are reading us? Remainder of my time, please, whoever feels qualified to answer that question.

Ms. MANFRA. Sir, first, I would offer that I think us and potentially some other agencies would be happy to come in and have a longer conversation about this, both quantum computing and other emerging technologies are definitely top of mind, not just our agencies, but many others. And I would argue that the U.S. Government is investing a lot in ensuring that we continue to maintain leadership in this space. And while, yes, we absolutely have to——

Mr. HIGGINS. So we can look forward to a SCIF [Sensitive Compartmented Information Facility] briefing on this?

Ms. MANFRA. Yes, sir, we will——

Mr. HIGGINS. I would ask the chairman to consider that.

Mr. LANGEVIN. Okay.

Mr. WILSON. And I would just add. I think quantum computing is at the core. Digital modernization at large, 5G, quantum computing, AI [artificial intelligence], large data or big data analytics, et cetera, are all converging. And so, in the Department of Defense, we see that as opportunity to field the right kinds of capability, both for productivity, but for effectiveness—mission effectiveness, but we also are looking at it through the lens of risk. So how do we mitigate that risk alongside our interagency partners?

We have the challenge of low-end and high-end conflict. And so, we have a reliance and we are becoming more reliant on those capabilities, so it is of utter importance. But we would love to join——

Mr. HIGGINS. Thank you. So we look forward to a more extensive briefing in a secure setting. Thank you, Mr. Chairman.

Mr. LANGEVIN. I thank the gentleman. Ms. Wasserman Schultz.

Ms. WASSERMAN SCHULTZ. Thank you, Mr. Chairman. Ms. Manfra, earlier this year CISA released a list of 56 national critical functions. You defined these as functions, quote, "so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, and national public health and safety." Is that correct?

Ms. MANFRA. Yes, ma'am.

Ms. WASSERMAN SCHULTZ. As it pertains to internet architecture, how does the identification of these 56 critical functions alter CISA's approach to protecting our Nation's internet infrastructure?

Ms. MANFRA. Thank you for the question, ma'am. What it does is more holistically defines what functions we are concerned about. So, previously, while it is important to continue to have these sector-specific approaches, but when we are talking to the IT community and the communications community, we felt it was important to narrow in a little bit more on what specifically. So are we talking about routing and addressing. Are we talking about the internet exchange point conversation and physical infrastructure that supports the internet.

So we felt it was important to start to disentangle so it is not just all, here is an IT and communications broad structure. Industry already thought this way. It was really us sort of catching up. And we will now shift how we prioritize our resources and our engagements to ensure that we have the right people in the room and we are taking the right actions against those critical functions.

Ms. WASSERMAN SCHULTZ. Thank you. And how does this change CISA's outreach and coordination with the private sector and with your partners at other agencies?

Ms. MANFRA. What it really means is we were going to ensure that the right players are in the room. We have great partnerships with the IT and communications industries, but as we started to think about a functional approach, which is, frankly, the way the adversaries are thinking about it, we recognize that not all of the correct players were in those conversations.

So, we want to ensure that the owners and the operators, the providers of services, are also a part of whether it is just information sharing back and forth so they can give us information about what may be going on, or we can provide them information. But also, they are part of this broader policy conversation when we are thinking about risks and what we want to do about it.

Ms. WASSERMAN SCHULTZ. Thank you. That list of national critical functions includes providing internet-based content information and communications services, and it also includes conducting elections. Is that correct?

Ms. MANFRA. Yes, ma'am.

Ms. WASSERMAN SCHULTZ. Of course, our internet architecture is connected to election security in many places across the country. So let me start by asking you a question that I have asked CISA Director Krebs multiple times since May of this year.

Russia intentionally influenced our 2016 elections and is expected to try again in 2020. Has the President received a comprehensive briefing from CISA on potential Russian influence in the 2020 elections?

Ms. MANFRA. My understanding is the President has received briefings and continues to receive briefings on threats.

Ms. WASSERMAN SCHULTZ. No, no, I am asking you, has he received a comprehensive briefing from CISA on potential Russian influence in the 2020 elections?

Ms. MANFRA. He has not directly received a briefing from us, but he has received comprehensive briefings that we have informed.

Ms. WASSERMAN SCHULTZ. Okay. That is new information because as that—since the last time I spoke with Director Krebs where he said no, or he was not aware that—small briefings here and there, that is different than a comprehensive briefing, specifically given to the President of the United States, on Russia's desire and intention to influence the 2020 election. So since the last time I asked him, that comprehensive briefing for the President of the United States has taken place?

Ms. MANFRA. Ma'am, to be honest, I am not in the meetings where the President receives these, but I do understand that the President has received multiple briefings on——

Ms. WASSERMAN SCHULTZ. Okay. So essentially, you are giving me the same answer that Director Krebs—he has not, to your knowledge, had a comprehensive briefing from CISA on this risk?

Ms. MANFRA. We have not directly provided him with briefing.

Ms. WASSERMAN SCHULTZ. Okay. Okay. Are there plans to brief the President on this critical issue in a comprehensive way from CISA?

Ms. MANFRA. I have would have to defer to others on that.

Ms. WASSERMAN SCHULTZ. And, lastly, are you familiar with the Quadrennial Homeland Security Review?

Ms. MANFRA. Yes, ma'am.

Ms. WASSERMAN SCHULTZ. That is a critical document that is used for assessing the Department's overall security strategy and what it views as the most pressing threats to U.S. security, including threats to critical infrastructure. Congress mandates that DHS produce this review every 4 years. Can you tell me the last time DHS submitted a Quadrennial Homeland Security Review to Congress?

Ms. MANFRA. Off the top of my head, I can't remember the exact year.

Ms. WASSERMAN SCHULTZ. It is 2013 or 2014.

Ms. MANFRA. Okay.

Ms. WASSERMAN SCHULTZ. And the most recent version of this document was due to Congress in December 2017, but more than 20 months later, DHS has not submitted this critical document. What is the status of the now long overdue 2018 Quadrennial Homeland Security Review?

Ms. MANFRA. Ma'am, I have to get back to you on that.

Ms. WASSERMAN SCHULTZ. Okay. If you could. The bottom line, Mr. Chairman, is not having an up-to-date Quadrennial Homeland Security Review makes it more difficult for Congress to evaluate DHS's strategy and coordinate with Federal agencies, which you very effectively answered on homeland security priorities, including our internet architecture.

So I would ask that you take it back to your bosses that it is time to comply with the law. And if you actually take this issue seriously, making sure that this report is issued in a timely fashion is essential. Thank you, I yield back.

Mr. LANGEVIN. I thank the gentlelady. And Mr. Waltz is recognized for 5 minutes.

Mr. WALTZ. Thank you, Mr. Chairman. Ms. Manfra, obviously, DHS defends the homeland and defends our critical infrastructure here, including our internet infrastructure. And Mr. Wilson, DOD, in a number of briefings, has described its posture now as defending forward in both classified and unclassified briefings, and I have received a number of briefings on what those activities have entailed, particularly as it pertained to 2018 and our elections there.

Is there any discussion in the Department—in the Defense Department, in particular amongst the interagency of moving to a deterrent strategy, rather than a purely defensive strategy, whether we are defending forward or defending the homeland. What I mean by that is, you know, to use as an analogy, terrorism.

We cannot bat 1,000, so to speak, using a baseball analogy. At some point, we have to alter our adversary's decision dynamic, and I think some members have described it as perhaps blinking the lights in the Kremlin or holding their assets at risk. What is the Department, from a policy standpoint, are they moving that direction? Have you made a decision not to move that direction, and we take a purely defensive posture? We could talk across a number of domains, obviously, where we have a deterrent strategy to stop and try and alter the behavior rather than simply defend against it. Does that make sense? And I would welcome your thoughts.

Mr. WILSON. Absolutely, sir. So last year, as part of our cyber posture review, we delivered a report to Congress, really hit two pieces. That was in early September. One was a holistic assessment of our ability to execute the missions as articulated in our DOD Cyber Strategy. So we did a gap assessment that is a classified report that we can make available.

In addition, we were asked to do some work on deterrence. Specifically, deterrence in cyberspace. And so a couple of the key takeaways: One, we believe that deterrence comes in a few flavors, it is not just consequences. We think the first step is deterrence by denial. So we want to deny adversaries the benefit of what they are trying to achieve through a cyber effects operation, or any other type of activity directed at the U.S., our allies, or the Nation at large. And so, that is where you see the partnership between DHS and the other departments and agencies of the U.S. Government, where we have stepped in and began to assist, enable, support the resiliency of our critical infrastructure segments. Not just focused on DOD systems, networks, weapon systems, et cetera. So our focus is much broader because we do rely and we see the importance of denying an adversary the benefit.

In addition, we look very hard at the ability, if called upon, to deliver consequences, not just kinetically, or in all the other domains of operation that the Department has, but also in the domain of cyberspace. And so, a lot of assistance from Congress with regards to some clarity on authorities. We have also in the strategy tried to articulate our role uniquely focused against external threats. And, in addition, the NSC team in the White House has led us and the interagency through a process with a new National Security Presidential Memorandum 13, which focuses on the decision process for either offensive or defensive cyber effects operations. The details of that we would have to go into a classified session, but that has been in play and I think just——

Mr. WALTZ. I would like to follow up and better understand that. And then also, better understand how that has been communicated to our adversaries, because obviously deterrence is only effective if they understand the consequences.

Mr. WILSON. Absolutely. So strategy, a clarity of authorities, and then the process for making decisions have been very key in the consequences part. In addition, we look at deterrence, really what I would describe as entanglement. So how do we entangle ourselves, or use and leverage one of our strengths as a Nation in the international arena?

So how do we bring alongside our close partners and operate together, and make the complexity of a targeting problem for an adversary more difficult. And then, lastly, how do we strategically communicate any actions we are taking across as a whole of government, not just the——

Mr. WALTZ. Just in the interest of time, I will take that for follow-up. Thank you and we will reach out to your staff. Very quickly. Who has—I know there was a question earlier, and I apologize if I am repeating it, on undersea cables. Who has authority on—or who has responsibility for defending undersea cables that directly affect the United States, its ability to communicate in our economy and international waters? It is just not clear to me, and if anyone wants to send that for the record, in the interest of time, Mr. Chairman, I believe my time is expired, I would appreciate it.

Ms. MANFRA. I think it would probably be best if we followed up with more details.

Mr. WALTZ. Thank you.

[The information referred to can be found in the Appendix on page 73.]

Mr. LANGEVIN. Ms. Stefanik.

Ms. STEFANIK. Thank you, Chairman Langevin. Mr. Wilson, my question is for you. With respect to helping secure our Nation's infrastructure and even responding to an incident or an attack upon our critical infrastructure, can you clarify the role that U.S. Cyber Command and U.S. Northern Command plays and the relationship between the two? What role does DISA play here? And are there clear chains of command so that these organizations and commands understand their particular role? Who is responsible for what? And then, how do they interface with DHS?

Mr. WILSON. So if there is an attack on the Nation that involves kind of a multi-domain attack, so kinetic strikes against the Nation, NORTHCOM [U.S. Northern Command] has the point. They have the lead for the defense of the Nation. So from a supporting/supported relationship, NORTHCOM is point. If there are activities that would require a cyber effects operations, or any type of response, Cyber Command would be in support of NORTHCOM in those instances.

If there is a unique, and it is a fairly contained, but very focused on a cyber security threat or activity, then there is a decision to be made, and in most cases, then we would look to Cyber Command to be the lead, and they would be the supported command, because it would be really contained within their purview, in direct coordination with and lots of communication and coordination so we are all on the same sheet of music.

So that activity, we have exercised that on many occasions, and that is maturing. I think if you had asked just a few years ago, that was a bit cloudy. I think we are doing great work in that front. Our Tier 1 exercises is beginning to really mature those relationships and the command and control activity that goes alongside those.

DHS is alongside in anything domestically along with FBI representation, and so, when required, if it is a domestic incident, there would be support either provided to DHS as part of our normal defense support to civil authorities, or DSCA roles, there is a mechanism to put that in play, and then we would institute that.

Ms. STEFANIK. Let me ask a more specific—let me use a more specific example. As we are heading towards 2020, obviously one of the focuses of every Member of Congress is making sure that we have secure resilient elections. And we are well-positioned to ensure that the lessons learned from 2016 in terms of our vulnerabilities that we are being offensive in terms of protecting our elections infrastructure.

So in that case, you know, let's say there are cyber effects, how does that responsibility—can you go through that decision-making process for that particular example. So online election system as part of a critical infrastructure, who is responsible for what?

Mr. WILSON. So we look at it through three really lines of effort, or lines of operation. The first is associated with election security infrastructure. So, in support of the DHS team, because they have purview, and so whether that is information, intelligence information sharing, activity directed at helping to secure, share any threats, any indicators of compromise, to make sure that the robust defenses that are in place to secure elections infrastructure. So that is kind of job one, if you will, for elections support.

The second line of effort we have within the DOD, and General Nakasone is at the helm here, is associated with disinformation, or malign influence. And so, FBI has point with regards to disinformation associated with elections or any other activity in the United States as a law enforcement activity. And, so, likewise, the combined team of U.S. Cyber Command and NSA [National Security Agency] would provide support to the FBI in the form of information sharing, any intelligence indicators we may have alongside the intelligence community. So we are one of many that would be supporting.

FBI does the vast majority of outreach to, like, social media to give them heads up that there is issues, that there is a threat associated with, you know, a malign actor, Russia or whoever, using social media to spread disinformation or try to sway the public as part of the elections, or just day to day.

And then, the last would be if we are called upon as a Department of Defense to deliver consequences in any form, whether it be cyber effects operations or anything else, then that is wholly within the Department of Defense, and we have the procedures, ma'am, as you have been briefed on with regards to the process for approval on those as part of the NSPM–13 [National Security Presidential Memorandum–13] process.

And so, we have executed some of those in the past, as you have been briefed, I can't get into details in this forum. So we are postured to be able to execute those types of operations in the future from an offensive or defensive activity. At times, we may partner with international partners, like we did during the 2018 election, and close partners and providing support in that arena, in what we would describe as hunt forward as part of our defend forward construct.

Those are the structures we have used that was very successful. We have gone in and looked at the after-actions and are tuning that, but we are well underway with all three of those lines of efforts for the 2020 elections.

Ms. STEFANIK. Yeah, I think fine-tuning that is going to continue to be important, because as you laid out, the infrastructure, the disinformation, and the third bucket, you have a lot of agencies who are in the mix, whether it is U.S. Cyber Command, NSA, DHS, FBI, so making sure that there is—DOD—there is a holistic approach and an understanding of who is responsible, because oftentimes, the attacks, and we saw this in 2016, it was multifaceted, it checked multiple boxes.

And thanks for the leniency. I yield back.

Mr. LANGEVIN. Excellent points. And it is one thing when we know the bad actor or what is coming; for example, we need to be prepared for the upcoming 2020 elections. And just as in 2018, we had a whole-of-government, whole-of-nation approach, we will do that again, I am confident, in 2020. The American people should know that.

It is the things that we can't anticipate coming up that—this is well-harmonized and the left hand knows what the right hand is doing. So it is going to be well thought-out, and it becomes muscle memory going forward.

Thank you, Ranking Member. Chairman Lynch is now recognized for 5 minutes.

Mr. LYNCH. Thank you very much. So we have about 2,600 internet companies, and I think there are no less than 90 undersea fiber cables that feed both the United States and its territories. The trend has been that those cables are clustered on a select number of landing stations. Is that clustering effect, even though it creates redundancy, I guess, because you got all these cables, which is good, the redundancy is good, but the vulnerability that that prevents is—excuse me, that that presents, is that a problem for us? Ms. Manfra.

Ms. MANFRA. I would say——

Mr. LYNCH. And by the way, the maps that show the cable are all publicly available, so I am not giving up any——

Ms. MANFRA. No, you are not, sir.

Mr. LYNCH [continuing]. National secrets there.

Ms. MANFRA. Most of what we actually see in the risks for some of the co-location and consolidation comes from natural hazards or accidents.

Mr. LYNCH. Okay.

Ms. MANFRA. And now that does also mean that other threats could potentially take advantage of that, and we have done—usually we are working jointly with the FBI, working to, you know, understand, do physical security assessments of those cable landing stations, helping the owners of those—of that particular infrastructure, improve both their physical security and the resilience, as well as——

Mr. LYNCH. Okay.

Ms. MANFRA [continuing]. Kind of how it gets passed from the cable landing station into sort of the rest of the internet ecosystem. So there is some—there is definitely concern around some of that consolidation, but it usually manifests itself when you have, say, a hurricane or something like that. So they have already built a lot of resilience into that to combat some of these natural disasters.

Mr. LYNCH. Okay. Let me just rephrase the question a little bit more generally. Do you repeatedly and continuously monitor and do threat assessments on individual aspects of our internet architecture?

Ms. MANFRA. Yes, sir, we do.

Mr. LYNCH. Once a year? Is that what we do it?

Ms. MANFRA. It depends. We do probably—I don't know that we would do any of them once a year. Many of these would be assessments that, ideally, they could use for multiple years, and would offer multiyear approaches to improving some of the security. But in some of the areas where we have maybe identified some weaknesses, or perhaps we have some threat intelligence that they may be a target, we do prioritize engagement, and we will continue to elevate the prioritization of those. I think this is really in the last few years that we have started to prioritize this.

Mr. LYNCH. Speaking very generally, what keeps you up at night? What do you worry about most when we look at the whole, you know, the scheme of our internet architecture? What do you think—and, again, being sensitive to the nature of the question, what do you think we should be doing to, you know, better protect ourselves?

Ms. MANFRA. When it comes to internet architecture, I think increased visibility, and working with those companies and ensuring resilience. There is a lot of talk about security, but I think resilience in this space, and it is already something that the community understands.

So having a lack of resilience, and whether that is through market pressures or others, would be a concern in that somebody could take advantage of that, and you would have single points of failure. I am not saying that we have that now, but that we would get to a point where we did, and the adversary would be able to have real, you know, catastrophic consequences as a result.

Mr. LYNCH. So the redundancy aspect of it, in many cases.

Ms. MANFRA. Oftentimes, resiliency through redundancy. There are other mechanisms for resiliency, but yes, redundancy, I think, is important.

Mr. LYNCH. Okay. Thank you very much.

I will yield back.

Mr. LANGEVIN. Thank you.

And on that point on the redundancy and the resiliency, obviously, things happen. There are physical failures. We talked about the anchor drags, and so, it is not the first time that a node has been damaged. And how quickly, give us a sense of how that can be reconstituted, or you have that resiliency, so you have another way of performing the same function through some other mechanism. And with that, also, how many points of failure then become on the scale of more catastrophic or serious, where resiliency is harder, and it takes longer?

Ms. MANFRA. I will take a stab at that, and then I can—so, it is hard to provide sort of one answer to that, because I think it depends on which part of it you are talking about. When you are talking about submarine cables, cable landing stations, internet exchange points, that part, you know, that is a knowable universe of who owns that; and so, it means it is also a little bit, I think, simpler, in terms of who we are engaging with and how we improve the security and the resilience.

You know, I think we have identified some really good best practices. And, honestly, industry has really led largely through telecommunications companies needing to build resilience in hurricanes, or whatever. So they have created mutual assistance agreements, essentially, in terms of when you are thinking about roaming. And if one company can't handle a customer set, because their infrastructure has gone down, they have agreements in place. And they have been doing this for a while. I think that is starting to evolve in broader than just these TELCOs [telephone companies], and that is something that we definitely welcome and want to encourage.

You also have to think about as the market is sort of—there are new players now coming into the market that didn't typically have cable landing stations or submarine cables. So how do we kind of think about these different market players, whether that is providing mutual assistance or the government ensuring that we prioritize?

We learned about this, whether it was, you know, Puerto Rico, Virgin Islands, some of these significant events in the Caribbean that had impact to critical nodes of our communications infrastructure. How do we ensure that working with FEMA [Federal Emergency Management Agency], that we are prioritizing the restoration of those services or we are helping industry prioritize the restoration of those services?

Ms. RINALDO. I think we often hear that the internet was not built with security in mind, but it was built upon to be resilient, and it is very resilient.

You know, a couple of things: With a routing cable, if there is a glitch, it can reroute traffic. It does reroute traffic. For the DNS system, DNS—NTIA represents the United States at ICANN [Internet Corporation for Assigned Names and Numbers] on these issues. We lead the DNS Interagency Working Group. There are the authoritative route servers, but there are also more than 1,000 route server instances, or anycasts, that are distributed all throughout the world. And this is done for security, for stability. It is done for the consumer.

So there are many instances that resiliency has been built into the system, and even to this day, we keep building and making sure that the system remains and is stable, because it is such a driver of our economic lives in this country as well as how we operate.

Mr. LANGEVIN. Mr. Wilson, do you have anything to add on that?

Mr. WILSON. Chairman Langevin, I would just add that, you know, just based on experience, the answer is it depends, in terms of a cable outage. If there is a cable outage at sea and you are, you know, a 2-day steam out to, you know, fix that cable, the diversity and the resiliency of the architecture can work around that.

As cables converge and if there is an incident like in a harbor or something, that may have more consequential outcomes. However, it is closer, so the remedy is typically quicker. In a lot of cases, it is just a physical restoration of services.

So the answer is, it depends. It can be very quick, a matter of hours. It can be several days, if not more, depending on the location and the type of fix action that is required. But I would just echo that these systems are built with resiliency.

Chairman Lynch, to your question, what is the threat? I think it would be the miscalculation of an adversary that is trying to seek or take—seek an outcome. It miscalculates with regards to how they go about doing it, the WannaCry-like incident that maybe has much more implications, worldwide or globally, than what an actor would have anticipated. That is what, I guess, keeps me up in the middle of the night.

Mr. LANGEVIN. So I want to just go back to the role of CYBERCOM and NORTHCOM in defending physical sites that are part of the internet architecture ecosystem. Do you have that worked out? And we have kind of touched upon that, but who has primary responsibility in defending those sites?

Mr. WILSON. So for the Department of Defense, we have very good knowledge about which systems we rely on. We have good plans in terms of mitigation with regards to moving to secondary or tertiary capability, whether that is cable systems or whatever portion of the architecture.

When it comes to defending—most of these are owned and operated by commercial vendors, in terms of these heavy-haul systems that we are talking about. So defending is a bit of a different question. It is the resiliency that is built in. But we understand our reliance, and if we need to take action to, if it is not happening naturally, is to be able to bring online other systems.

Many times for the Department, that may be prioritization of mission. In other words, we may have to go without that broadband or that very large bandwidth support in terms of comms. We may have to go to a much more minimized posture. We understand how to do that, and we have moved to that contingency action, set of actions. That is part of how we do business day in and day out.

Mr. LANGEVIN. Thank you.

I guess the last question that I will have is for Ms. Rinaldo. Given NTIA's role in international standards bodies, can you speak to how this issue is viewed by other countries and your international counterparts?

Ms. RINALDO. Thank you for the question. Yes. We represent the United States at ICANN, as well as we are very active in standards bodies 3GPP [Third Generation Partnership Project], IETF [Internet Engineering Task Force], as well as others, ITU [International Telecommunication Union], which is the telecommunications arm for the U.N [United Nations]. We have great allies around the world. We coordinate with them often. We coordinate with them through different conferences as well as bilats throughout the course of the year. We want to make sure that as we face threats to our infrastructure, threats to the networks, that we are speaking with one voice and making sure that we are pushing back.

There are more of us than them, so we want to make sure that we continue these conversations, so when foreign adversaries do pose threats, that we keep having those lines of communication open. And these four that do occur around the world, it is an amazing opportunity to not only exchange notes, but to further deepen those bonds.

Mr. LANGEVIN. Thank you.

With that, Mr. Higgins is now recognized for 5 minutes.

Mr. HIGGINS. Thank you, Mr. Chairman.

Mr. Wilson, if a United States Navy ship is fired upon by an identified approaching vessel, an aggressor, do we return fire?

Mr. WILSON. There are standard rules of engagement regarding——

Mr. HIGGINS. Yes, sir.

Mr. WILSON. Absolutely.

Mr. HIGGINS. If a soldier in a theater of engagement is fired upon by an identified aggressor, do we return fire?

Mr. WILSON. Yes.

Mr. HIGGINS. Ms. Manfra, do you see the comparison? So please explain to America what the difference of our policy is when we come under cyberattack, our policy regarding preemptive attack, or our policy regarding return fire. If the aggressor can be identified, there is a growing consensus on the part of that group that if we can identify these guys, why don't we strike back?

Ms. MANFRA. Well, sir, I think the Department of Defense is doing a lot of work to be well-postured and to do just that. I think it is important, though, to not conflate every cyber incident as having the same consequences, shooting on one of our sailors or soldiers.

Mr. HIGGINS. Why not? If we come under cyber fire, why would we not return cyber fire?

Ms. MANFRA. I would say two things: Cyber fire, it could often just be a—it could be a data breach. I would argue that that is not an act of war. That is why we focus so much on the consequences.

Mr. HIGGINS. Well, let's talk about that with America for a moment.

Ms. MANFRA. Okay, sir.

Mr. HIGGINS. If a database—let's refer to it as that—comes under missile attack, is that an act of war? If it is destroyed by a missile that is an act of war, but if it is destroyed by cyber, that is not? These are legitimate questions.

Ms. MANFRA. A very legitimate question, sir, and one that a lot of people are thinking very hard about. I just—I would say——

Mr. HIGGINS. Let me compare it to sniper fire.

Ms. MANFRA. From my perspective, sir——

Mr. HIGGINS. Like returning sniper fire, very targeted return fire.

Ms. MANFRA. We have a long history of defining what it means to escalate and to have an act of war. And the digital, sort of, modernization of our economy has forced us to think differently about that. I don't want to suggest that we are not returning fire when we are attacked. I only mean to suggest that it is important to understand what the consequences are that they are achieving and that we use the right tools.

It is not always necessary to return a cyber fire, as you said, sir, with a cyber gun. There are many other tools that the government has and does use, but I think one of the things that I am proudest of is the work that we are doing with DOD to ensure that both of us are postured and positioned to not only defend what we can domestically, but so that DOD is better postured to take such actions.

Mr. HIGGINS. Very well. That was an intelligent answer. Let me just close by saying that America is not accustomed to hiding when we come under fire. And Americans watching right now, they think we are returning fire, and we are largely not, not to the standards that it is common knowledge that if a Navy ship comes under fire, that other ship is about to get something back.

Ms. MANFRA. Yes, sir.

Mr. HIGGINS. If a soldier comes under fire, we are going to return that with superior fire and training. But cyberattack is legitimate, is dangerous. It threatens our commerce, our industry, our grid, our internet infrastructure, our military, our financial institutions. It is certainly a legitimate threat. We are talking about it today. And America expects us to return fire.

Ladies and gentlemen, sir, thank you for being here today.

Mr. Chairman, I yield.

Mr. LANGEVIN. I thank the gentleman.

I want to thank all of our witnesses for your testimony today. Members may have additional questions, and we would ask that you be responsive in answering those questions and submitting them to the committee.

Again, I want to thank you for the important topics we have discussed today. The answers—obviously, this is going to be an ongoing dialogue. It is something we have to pay continued attention to. I also just want to thank Chairman Lynch and Ranking Member Stefanik and Ranking Member Hice for their participation and support of this hearing.

I yield to Mr. Lynch for any final comments that he would like to make before we adjourn.

Mr. LYNCH. I think these witnesses have suffered enough. I think we should probably let them go.

Mr. LANGEVIN. Very good. I thank you all for being here and what you do on behalf of the country.

This meeting stands adjourned.

[Whereupon, at 4:42 p.m., the subcommittees were adjourned.]

APPENDIX

SEPTEMBER 10, 2019

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

SEPTEMBER 10, 2019

Opening Statement
Chairman James R. Langevin
Intelligence and Emerging Threats and Capabilities Subcommittee

Securing the Nation's Internet Architecture

September 10, 2019

The subcommittee will come to order. I am pleased to welcome everyone to a joint hearing with the Committee on Oversight and Reform's Subcommittee on National Security about the security of the nation's internet architecture. I am particularly thankful to my friend Mr. Lynch and his staff for working so diligently in making today possible.

We are here to conduct overdue oversight regarding the security of the internet's underlying architecture—namely the components, physical sites, and assets that are necessary for the internet to operate. Defending the United States' assets in this global telecommunications networks requires a whole-of-nation approach, and I am concerned that the government is not approaching the subject in a cohesive or comprehensive manner, creating significant risk for the nation. Both the Oversight and Armed Services Committees are seeking a better understanding of the policies, regulations, guidelines and interagency agreements that govern the protection of this critical infrastructure. To the extent there are gaps, we are also interested in learning whether legislative solutions may be needed.

Most people think of the internet as the they visit, the applications they use, and the emails they send. In other words, people's understanding of what the internet is tied to how they engage with it. However, this leaves out an entire architecture that enables the flow of information around the world and into people's palms. This architecture includes the high-capacity cables buried under the ground and laid below the sea, the cable landing stations that connect the cables from continent to continent, and internet exchange points (IXPs) that serve as clearinghouses for data between Internet Service Providers (ISPs) and content delivery networks (CDNs). These are all examples of physical sites and tangible items that are required for the internet to operate.

While these physical sites are critical components of the cyber landscape, they are generally viewed as distinct from the networks, protocols, and software that are more familiar to people's understanding of the internet. However, they are just as important to internet operations. After all, unplugging a network cable is just as effective a denial of service attack.

From the government's perspective, tackling the subject of internet architecture security is difficult due to departments and agencies' overlapping jurisdictions, responsibilities, and capabilities. I am concerned that the Executive Branch has fragmented internet architecture security among multiple departments, as opposed to conceptualizing the intemet as a single ecosystem with departments working collaboratively.

For example, the Department of Homeland Security (DHS) serves as government lead for all critical infrastructure, and as the sector-specific agency for the telecommunications sector. Meanwhile, the Department of Commerce's National Telecommunications and Information Administration (NTIA) is principally responsible for advising the President on telecommunications and information policy issues, and develops national policies on intemet use and cybersecurity. Separately, the Department of Defense (DoD) is broadly responsible for defense of the nation. Independent regulatory agencies, like the Federal Communications Commission (FCC), also have important responsibilities for ensuring security.

I have no doubt that these agencies work together broadly, however I am very worried that by carving out discreet lanes in the road, there are seams left unaddressed in the middle, and am concerned that internet architecture security is one of those seam issues. Holistic intemet architecture security has been generally neglected, with organizations remaining firmly in their lanes rather than approaching the problem collectively.

Our nation's newest cybersecurity organization, the Cybersecurity and Infrastructure Security Agency, has recognized the inherent challenges in using a critical infrastructure sector framework, particularly with respect to interdependencies between sectors. The National Risk Management Center's National Critical Functions Set explicitly recognizes intemet architecture functions, such as "Operate Core Network" and "Provide Internet Routing, Access, and Connection Services." I am hopeful that this new framing will help stimulate more cross-agency—and cross-sector—discussion, interaction, and policy development.

The purpose of today's hearing is to better understand how the interagency is approaching internet architecture security, including with respect to engagement with the private sector. In particular, I will be interested in hearing from the witnesses how their agencies deal with the fact that internet architecture security is not purely a "cyber problem" and it is not purely a "physical problem". In order to effectively reduce our risk, DoD will have to actively engage non-security centric agencies such as NTIA and regulatory bodies such as the Federal Communications Commission, and vice versa. Our country's cyber experts will have to sit down with specialists in physical security and electrical distribution professionals, because at the end of the day, it won't matter if these sites and systems are taken offline by cyber attack, sabotage, or natural disaster.

There is no greater sign of how cross-cutting this issue is than the fact that the IETC Subcommittee is joined today by the Oversight Committee's National Security Subcommittee. Even within the House of Representatives, we are inclined to handle things within caucuses or within committees, but in recognition of the problem's scale, we are here tackling this together, because that's exactly what it

With that, I will turn first to Ranking Member Stefanik and then to Chairman Lynch and Ranking Member Hice for their remarks.

Testimony

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

FOR A HEARING ON

"Role of the United States Government in Securing the Nation's Internet Architecture"

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES

Committee on Armed Services, Subcommittee on Intelligence and
Emerging Threats and Capabilities
Committee on Oversight and Reform, Subcommittee on National Security

September 10, 2019

Washington, DC

Chairman Langevin, Chairman Lynch, Ranking Member Stefanik, Ranking Member Hice and members of the Subcommittees, thank you for today's opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) ongoing and collaborative efforts to secure the Nation's internet architecture. Safeguarding cyberspace is a core homeland security mission, and CISA leads the Nation's efforts to advance the security and resilience of our cyber infrastructure.

CISA is responsible for assisting agencies with protecting civilian Federal Government networks and coordinating with other federal agencies, as well as state, local, tribal, and territorial governments, and the private sector to defend our Nation's critical infrastructure. We work to enhance information sharing across the globe in order to help critical infrastructure entities and government agencies protect their infrastructure, and we do this in a way that protects privacy and civil liberties. By bringing together all levels of government, the private sector, international partners, and the public, CISA strengthens the resilience of our Nation's critical infrastructure.

Risk Characterization

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. We have seen advanced persistent threat actors, including hackers, cyber criminals, and nation-states, increase the frequency and sophistication of their attacks. In a 2018 report, *Foreign Economic Espionage in Cyberspace,* the U.S.'s National Counterintelligence and Security Center stated, "We anticipate that China, Russia, and Iran will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace." Our adversaries have been developing and using advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democratic institutions.

The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. According to the U.S. Department of Commerce's Bureau of Economic Analysis, the digital economy supported 5.1 million jobs and accounted for $1.4 trillion of gross domestic product (GDP) in 2017, or about 7 percent of the U.S. economy. Virtually every element of modern life is now dependent on cyber infrastructure. The sector recognizes that other sectors consider its services to be critical, and its practices reflect this understanding.

The nature of communication networks involve both physical infrastructure (buildings, switches, towers, antennas, etc.) and cyber infrastructure (routing and switching software, operational support systems, user applications, etc.), representing a holistic challenge to address the entire physical-cyber infrastructure. The result has been the establishment of a robust, resilient network infrastructure that successfully provides services globally. Over the last several decades, the sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry, using terrestrial, satellite, and wireless transmission systems.

CISA Roles and Responsibilities

CISA, along with the Department of Defense (DOD), Department of Commerce, and other government and private sector partners, engage in a strategic and unified approach towards improving our nation's overall defensive posture against malicious cyber activity. In May of 2018, the DHS published the *DHS Cybersecurity Strategy*, outlining a strategic framework to execute our cybersecurity responsibilities during the next five years. The *National Cyber Strategy*, released in September 2018, reiterates the criticality of collaboration and strengthens the government's commitment to work in partnership with industry to combat cyber threats and secure our critical infrastructure. Together, the *National Cyber Strategy* and *DHS Cybersecurity Strategy* guide CISA's efforts.

The private sector, as owners and operators of the majority of communications infrastructure, is the primary entity responsible for protecting sector infrastructure and assets. Working with the Federal Government, the private sector is able to predict, anticipate, and respond to sector outages and understand how they might affect the ability of the national leadership to communicate during times of crisis, impact the operations of other sectors, and affect response and recovery efforts.

A core component of the CISA mission is advancing reliable and secure communications for public safety, critical infrastructure owners and operators, and the general public. CISA supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient. We assist with preparedness by ensuring federal, state, local, tribal and territorial public safety organizations have the necessary plans, resources, and training needed to support operable and advanced interoperable emergency communications. Additionally, CISA works across government and industry to ensure the national security and emergency preparedness community has access to priority telecommunications and restoration services to communicate under all circumstances.

CISA serves as the Sector-Specific Agency (SSA) for the Communications and Information Technology Sectors, and it operates the Communications Sector Information Sharing and Analysis Center. We lead communications response and recovery efforts under Emergency Support Function 2 of the National Response Framework. Through our operations center, we monitor national and international incidents and events that may impact communications infrastructure. Today, 11 Federal Government agencies and more than 60 private sector communications and information technology companies routinely share critical communications information and advice in a trusted environment to support CISA's national security and emergency preparedness communications mission. As the SSA for these sectors, DHS works closely with DOD, Department of Justice, Department of Commerce, Federal Communications Commission, General Services Administration, the Intelligence Community, and the private sector to address both short-term and longer-term challenges regarding risks to telecommunications networks.

CISA shares timely and actionable classified and unclassified information, focusing on sharing cyber threat information in a manner that protects privacy and civil liberties, and the confidentiality of those who share sensitive information with us. CISA also provides training and technical assistance. Our work enhances cyber threat information sharing between and among governments and businesses across the globe to stop cyber incidents before they occur and quickly recover when they do. By bringing together the intelligence community, law enforcement, DOD, Sector-Specific Agencies, all levels of government, the private sector, international partners, and the public, we are enabling collective defense against cybersecurity risks, improving our incident response capabilities, enhancing information sharing of best practices and cyber threats, strengthening our resilience, and facilitating safety.

CISA provides entities with information, technical assistance, and guidance they can use to secure their networks, systems, assets, information, and data by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. CISA operates at the intersection of the Federal Government, state and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities. The *Cybersecurity Information Sharing Act of 2015* (P.L. 114-113) established DHS as the Federal Government's central hub for the sharing of cyber threat indicators and defensive measures. CISA's automated indicator sharing capability allows the Federal Government and private sector network defenders to share technical information at machine speed.

Joint DOD and DHS Cybersecurity Efforts

The challenge of effectively coordinating homeland security and homeland defense missions is not new, but it is amplified and complicated by the global, borderless, interconnected nature of cyberspace where strategic threats can manifest in the homeland without advanced warning. Almost a year ago, DHS and DOD finalized an agreement, which reflects the commitment of both Departments in collaborating to improve the protection and defense of the U.S. homeland from strategic cyber threats. This agreement clarifies roles and responsibilities between DOD and DHS to enhance U.S. government readiness to respond to cyber threats and establish coordinated lines of efforts to secure, protect, and defend the homeland.

The roles and responsibilities of DOD and DHS are complementary, but different. DOD must maintain the U.S. military's ability to fight and win wars and project power in a contested environment or while under attack in any domain, including cyberspace. As the government lead for national risk management, DHS is responsible for leading overall government efforts to protect critical infrastructure and civilian federal government informational system. As a part of these missions, DHS is working with a range of partners to identify national critical functions and ensure their integrity and resilience by leading government efforts to integrate and coordinate cybersecurity risk management and assistance with state, local, tribal, and territorial, and private sector critical infrastructure partners. DHS is a focal point for sharing cyber threat indicators and information and is responsible for providing tools, services, and programs to reduce and mitigate the risk of catastrophic consequences stemming from cyber-attacks.

DHS and DOD are both committed to improving the protection and defense of the homeland from strategic cyber threats. Specifically, DHS and DOD are working to improve intelligence, indications, and warning of malicious cyber activity; strengthen the resilience of the highest priority national critical infrastructure; improve joint operations planning and coordination; improve joint incident response to significant cyber incidents; expand cooperation with State, local, tribal and territorial authorities; and improve joint defense of Federal networks.

DHS and DOD will achieve these objectives through three primary lines of effort. First, DOD and DHS are adopting a threat-informed, risk-based approach that ensures the resilient delivery of national critical functions and services, and denies strategic adversaries the ability to prevent delivery of such functions and services. DOD and DHS will jointly prioritize a set of high priority national critical functions and non-DOD owned mission critical infrastructure that is most critical to the military's ability to fight and win wars and project power. Second, DOD and DHS, in coordination with the FBI and the intelligence community, are collaborating to build a common understanding of strategic cyber threats that can empower private sector network defenders, critical infrastructure owners and operators, and government actors to improve resilience and integrity of national critical functions. Timely access to threat information related to adversary capabilities and intent is critical to understand and counter the risk facing our nation's critical infrastructure effectively. Third, DOD and DHS are coordinating to inform and mutually support respective planning and operational activities as appropriate for each Department's unique authorities. DHS's knowledge of the domestic risk landscape, its work with the private sector, can inform DOD's efforts to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure. And, DOD's "defend forward" operations can inform and guide DHS efforts to anticipate adversary action and understand potential risks to critical infrastructure.

5th Generation Mobile Communications

Advances in 5G technology, the Internet of Things (IoT), and other emerging technologies are driving significant transformation in how we communicate, operate our critical infrastructure, and conduct economic activity. 5G is the next generation of networks that will enhance the bandwidth, capacity, and reliability of mobile communications. 5G was launched on a limited-basis in the United States and South Korea at the end of 2018, and more countries are rolling it out this year. According to the Global System for Mobile Alliance (GSMA), 5.1 billion people, or 67 percent of the global population, are subscribed to mobile services. It is expected that 5G networks will cover 2.7 billion people, or 40 percent of the global population, by 2025.

The first generation of wireless telecommunications networks in the United States was deployed in 1982, and its capabilities were limited to basic voice communications. Later generations added capabilities like text, picture, and multimedia messaging; Global Positioning System (GPS) location; video conferencing; and multi-media streaming. 5G networks will support greater bandwidth, capacity for tens of billions of sensor and smart devices that make up IoT, and ultra-low latency necessary for highly-reliable, critical communications. According to GSMA, between 2018 and 2025, the number of global IoT connections will triple to 25 billion. Autonomous vehicles, critical manufacturing, medical doctors practicing remote surgery, and a smart electric grid represent a small fraction of the technologies and economic activity that 5G will support. With these dramatic advancements in telecommunications and technologies associated with them also comes increased risk to the Nation's infrastructure.

Risks to mobile communications generally include such activities as call interception and monitoring, user location tracking, attackers seeking financial gain through banking fraud, social engineering, ransomware, identity theft, or theft of the device, services, or any sensitive data. Integrating 5G into current wireless networks may convey existing vulnerabilities and impact 5G network security. The capabilities 5G will allow for ensures exponentially more data will be transmitted to, from, and across networks. Data on 5G networks will flow through interconnected cellular towers, small cells, and mobile devices that may provide malicious actors additional vectors to intercept, manipulate, or destroy critical data. Due to the nature of 5G network architecture, many more pieces of cellular equipment will be present in the physical world. Malicious actors could introduce device vulnerabilities into the 5G supply chain to compromise unsecured wireless systems and exfiltrate critical infrastructure data. 5G technology will enable significant advances in our society and the prosperity of the U.S. but will also usher in an age of significantly greater cyber vulnerability.

Undersea Cables

An unclassified joint paper released in 2017 by DHS and the Office of the Director of National Intelligence – in coordination with the private sector – examined the risks to undersea cables and landing stations and potential avenues to mitigate such risks. Undersea cables transmit more than 97 percent of the world's electronic communications and pose potentially devastating consequences in the event of failure. In addition to accidental physical threats, there are vulnerabilities relating to nation-state adversaries, cyberterrorists, hactivitists, and cybercriminals.

Domain Name Service

In January 2019, CISA issued Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*, directing Federal civilian agencies to take a series of immediate actions in response to a global Domain Name System (DNS) hijacking campaign. This was the first Emergency Directive issued by CISA under authorities granted by Congress in the Cybersecurity Act of 2015. The action took place after carefully considering the current and potential risk posed to Federal agencies.

The FY 2020 President's Budget also includes funds to begin development efforts to centralize the authoritative DNS resolution services for the Federal Government. The managed service will provide centralized DNS management for the Federal Government and a rich set of analytics that sit on top of traditional DNS services.

Conclusion

In the face of increasingly sophisticated threats, CISA employees stand on the front lines of the Federal Government's efforts to defend our Nation's federal networks and critical infrastructure. The threat environment is complex and dynamic with interdependencies that add to the challenge. As new risks emerge, we must better integrate cyber and physical risk in order to effectively secure the Nation. CISA contributes unique expertise and capabilities around cyber-physical risk and cross-sector critical infrastructure interdependencies.

I appreciate the Subcommittees' strong support and diligence as it works to understand this emerging risk and identify additional authorities and resources needed to address it head on. We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure, and resilient Homeland through our efforts to defend today and secure tomorrow.

Thank you for the opportunity to appear before the Subcommittees today, and I look forward to your questions.

Jeanette Manfra

Jeanette Manfra serves as the Assistant Director for Cybersecurity for the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Ms. Manfra leads the Department of Homeland Security (DHS) mission of protecting and strengthening the nation's critical infrastructure from cyber threats.

Previously, Ms. Manfra served as Assistant Secretary for the Office of Cybersecurity and Communications (CS&C) for the National Protection and Programs Directorate (NPPD) before the agency became CISA on November 16, 2018. Prior to this position, Ms. Manfra served as Acting Deputy Under Secretary for Cybersecurity and Director for Strategy, Policy, and Plans for NPPD.

Ms. Manfra also served as Senior Counselor for Cybersecurity to the Secretary of Homeland Security and Director for Critical Infrastructure Cybersecurity on the National Security Council staff at the White House.

At DHS, she held multiple positions in the Cybersecurity Division, including advisor for the Assistant Secretary for Cybersecurity and Communications and Deputy Director, Office of Emergency Communications, during which time she led the Department's efforts in establishing the Nationwide Public Safety Broadband Network.

Before joining DHS, Jeanette served in the U.S. Army as a communications specialist and a Military Intelligence Officer.

Last Published Date: November 28, 2018

TESTIMONY OF DIANE RINALDO

ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION (ACTING)

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
(NTIA)

U.S. DEPARTMENT OF COMMERCE

HOUSE ARMED SERVICES SUBCOMMITTEE ON INTELLIGENCE AND EMERGING
THREATS AND CAPABILITIES AND HOUSE OVERSIGHT AND REFORM
SUBCOMMITTEE ON NATIONAL SECURITY

U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 10, 2019

Chairman Langevin, Chairman Lynch, and Members of the Committee:

Thank you for this opportunity to testify today on the role of the U.S. government in securing the nation's Internet architecture.

The National Telecommunications and Information Administration (NTIA) in the Department of Commerce is responsible for advising the President on telecommunications and information policy. NTIA's programs and policymaking focus on a broad range of issues that include spectrum management and availability, broadband connectivity, and the growth and stability of the Internet. NTIA also is the agency charged with oversight of FirstNet, the independent authority within NTIA that is tasked with ensuring the development, building, and operating of the nationwide broadband network that equips first responders with essential digital tools that help save lives and protect U.S. communities.

During a time when an ever-changing landscape of services, technologies, and global actors are seeking to influence the Internet's future, NTIA collaborates with other Commerce bureaus and Executive Branch agencies to develop and advocate for domestic and international policies that preserve the open Internet and advance key U.S. interests. NTIA coordinates Executive Branch communications activities and represents the Administration's policies before the Federal Communications Commission (FCC).

The Nation's telecommunications infrastructure is the physical medium through which all Internet traffic flows. It underpins the foundation of our digital economy. NTIA's role is to foster national safety and security, economic prosperity, and the delivery of critical public services through telecommunications. In this capacity, NTIA is involved in numerous policy issues that affect the security of critical elements of our Nation's telecommunications infrastructure, encompassing exchange points, data centers, content delivery networks, the domain name system, undersea cables, and cable landing stations, as well as the diverse array of communications access networks and technologies that enable American consumers, businesses, and other institutions to connect to the Internet.

Our support includes working with our interagency partners to enhance the security of our Nation's telecommunications supply chain, advocating the United States' longstanding policy against data localization regimes, and participating in Executive Branch reviews of applications before the FCC that involve transactions with a significant foreign ownership component. We also are supporting the Secretary of Commerce as needed on the implementation of the Executive Order on Securing the Information and Communications Technology and Services Supply Chain.

NTIA is also the Executive Branch expert agency on issues relating to the Domain Name System (DNS), a critical component of the Internet infrastructure. The DNS functions similar to an "address book" for the Internet by allowing users to identify websites, mail servers, and other Internet destinations using easy-to-understand names (e.g., www.ntia.gov) rather than the numeric network addresses (e.g., 198.51.11.177) to look up information on the Internet. NTIA supports a multistakeholder approach to the coordination of the DNS to ensure the long-term viability of the Internet as a force for innovation and economic growth.

5G Security

The United States is dependent on reliable access to the finite resources that is radiofrequency spectrum. As with any critical resource, access to spectrum must be managed efficiently and effectively in order to achieve key economic and national security goals of the United States including the deployment of 5G networks and that our federal spectrum users, such as the Federal Aviation Administration (FAA), can operate its radio operations free from receiving harmful interference. As management of spectrum licenses or authorizations becomes more automated and networked, the security of the information systems utilized becomes even more essential and NTIA will work to ensure that it continues to manage risk to these essential systems.

NTIA is a regular participant in the 3rd Generation Partnership Project (3GPP), which unites seven telecommunications standards development organizations from across the world and provides their members with a stable environment to produce the reports and specifications that define the 3GPP technologies behind today's ubiquitous mobile wireless networks and the emergence of 5G. 3GPP addresses cellular technologies, including radio access, security, core network and service capabilities that provide a complete system description for mobile telecommunications.

The Domain Name System

NTIA leads a longstanding interagency working group dedicated to matters pertaining to the Domain Name System (DNS). This DNS interagency working group includes representatives from the Department of Justice, Federal Bureau of Investigations, Department of Defense, Food and Drug Administration, Department of State, Department of Homeland Security (DHS), Internal Revenue Service, Department of the Treasury, U.S. Postal Service, U.S. Patent and Trademark Office, Secret Service, Security and Exchange Commission, the National Institute of Standards and Technology (NIST), and others. Through this interagency group, NTIA informs and coordinates with relevant agencies on matters pertaining to the security, stability, and resiliency of the DNS.

NTIA also oversees the management of the .us and .edu domains. In this role, NTIA coordinates responses to DNS incidents that pertain to these domains. Specific to .us, there are requirements associated with securing the name space and making it a safe and reliable domain. Under NTIA's oversight, both .us and .edu have implemented DNSSEC and employed other security and stability measures, and modernized their operations in a manner that improves the overall security of their domain space.

NTIA has a well-established relationship with the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a not-for-profit, public-benefit organization that oversees the operation of the Internet's DNS, coordinates allocation and assignment of the Internet's unique identifiers, such as Internet Protocol addresses, accredits generic top-level domain name registrars, and helps facilitate the voices of stakeholders worldwide who are dedicated to keeping the Internet secure, stable and interoperable.

NTIA was a leader in the creation of ICANN that evolved over the years through a series of legal agreements and contracts, and engages with ICANN and the broader global community on matters that are specific to ensuring the continued security, stability, and resiliency of the

DNS. Per statute, NTIA represents the U.S. Government in ICANN's Governmental Advisory Committee (GAC), which advises ICANN on public policy issues related to the Internet DNS. NTIA coordinates with other governments and stakeholders on domain name related security matters. For example, NTIA engaged the DNS interagency working group as well as Federal Chief Information Officers in preparation for the first-ever changing (rolling) of the DNS Security (DNSSEC) cryptographic key at the authoritative DNS root that took place in October 2018. NTIA will continue to work with agencies as well as other domestic and international partners in promoting DNSSEC implementation. Overall, NTIA's relationship with ICANN has proven useful in information exchange and coordinated response on all matters related to the DNS, including DNS based cyber incidents, DNS abuse, and strengthening the overall security of the DNS.

Supply Chain

The telecommunications infrastructure is critical to nearly every aspect of the American economy and national security. The complex global telecommunications supply chain is increasingly vulnerable due to the proliferation of some foreign-sourced products and services. One way NTIA helps address these challenges is by supporting the Secretary of Commerce in implementing the President's Executive Order on Securing the Information and Communications Technology and Service Supply Chain. NTIA also serves as a member of the executive committee of DHS's Information and Communications Technology (ICT) Supply Chain Risk Management Task Force, which provides advice and recommendations to DHS and private sector owners and operators of ICT critical infrastructure about how to assess and manage risks associated with the ICT supply chain. Finally, NTIA strongly supports the recently updated version 1.1 of the NIST Cybersecurity Framework, which incorporates a new section helping organizations understand and manage supply chain risks.

FirstNet

Congress created the First Responder Network Authority (FirstNet) in the Middle Class Joh Creation and Tax Relief Act of 2012 (P.L. 112-96) with the duty to ensure the deployment, operation, and maintenance of the nationwide public safety broadband network (FirstNet network), to address the lack of a standardized interoperable communications platform for first responders. The critical nature of first responders' communications demands that the network must be resilient and provide high availability, security, and privacy protections.

Cybersecurity is critical to the FirstNet mission to ensure all components of the FirstNet network are secure, reliable, and work together to provide first responders the data and communications they need on time, intact, and secure. From its inception, the FirstNet network has incorporated end-to-end cybersecurity for the network and its users. In partnering with AT&T, FirstNet invested years of planning and experience to create a secure environment for first responders. Among the key components of the enhanced cybersecurity of the FirstNet network design is the nationwide dedicated core network implemented by AT&T.

FirstNet network subscriber traffic running through the dedicated core ensures higher levels of reliability, redundancy, and protection through the dedicated processing and routing of the public safety traffic. Another critical enhancement can be found in the dedicated Security Operations Center (SOC), which handles continuous monitoring, detection, and mitigation efforts in cybersecurity for the network. The SOC provides 24/7/365 coverage and support for all cybersecurity considerations, and is backed up by the full global network visibility of AT&T to ensure proactive protection for public safety.

From a cross functional perspective, all aspects of cybersecurity are evaluated and reviewed within the context of the FirstNet network. This includes user equipment, such as phones, tablets, and in-vehicle routers, and anything that is connected to the network, such as the Internet of Things (IoT). Similarly, there are processes in place for the vetting and inclusion of software applications developed for the public safety market.

Interagency Collaboration

NTIA collaborates across the U.S. Government on numerous efforts related to the security of the nation's Internet architecture. We have been working closely with the National Security Council (NSC) and our interagency colleagues on implementing the National Cyber Strategy, which just marked its one-year anniversary. In that effort, we shared our activities across the interagency and looked for synergies to maximize the impact of the strategy. NTIA will continue to participate in these efforts.

NTIA is engaged in numerous interagency efforts aimed at securing and increasing the resiliency of satellite systems, including representing executive branch equities on the encryption of telemetry, tracking, and command (TT&C) links and the development of policy guidance to help the owners and operators of critical infrastructure in their use of Global Positioning Systems (GPS) services.

Botnet Coordination

One significant example of NTIA's contribution to the protection of the Internet infrastructure is our work with NIST and DHS on the Botnet Report, delivered to the President in May 2018 in response to Executive Order 13800. Botnet attacks can have large and damaging effects, and they put the broader network at risk. The usual distributed denial of service (DDoS) mitigation techniques, including network providers building in excess capacity to absorb the effects, are designed to protect against botnets of a certain size. But much bigger botnets now capitalize on the sheer number of Internet of Things (IoT) devices. We have seen attacks that have topped a terabit per second. Dealing with a DDoS attack of this magnitude can take time, which is a major concern when mission-critical services are involved. Risks will increase as connected devices continue to proliferate.

The Botnet Report outlines a positive vision for the future, cemented by six principal themes and five complementary goals that would improve the resilience of the Internet ecosystem. For each goal, the report suggests supporting actions that can be taken by both government and the private sector. The Departments of Commerce and Homeland Security developed the report through an open and transparent process for the specific purpose of identifying stakeholder actions as opposed to government regulations.

We are tracking progress through a document known as the Botnet Road Map. More than half of the identified tasks are already in progress or completed. Some of our private sector partners have already moved forward with supportive initiatives. For example, the Council to Secure the Digital Economy published its first International Anti-Botnet Guide late last year.

Remediating botnet threats is an ecosystem-wide challenge that will take time to accomplish – we recognize that botnets are not going to be “solved” in one year. At the end of this year, the Departments of Commerce and Homeland Security will provide a status update to the President that reviews progress, tracks the impact of the road map and sets further priorities.

Cybersecurity Multistakeholder Processes

NTIA’s cybersecurity multistakeholder processes contribute to the security of the nation’s Internet architecture. Our ultimate objective is to foster a more resilient ecosystem through the creation of industry-led, market-based cybersecurity solutions.

Most recently, NTIA has been working on software component transparency. Most modern software is not written completely from scratch, but includes existing components, modules, and libraries from the open source and commercial software world, which can be challenging to track. The IoT compounds this phenomenon, as new organizations, enterprises and innovators take on the role of software developer to add “smart” features or connectivity to their products. The sheer quantity of software inputs means that some products ship with vulnerable or out-of-date components.

NTIA convened a multistakeholder process late last year between software vendors and the enterprise customer communities who use these products. Stakeholders have talked to industry and government experts across the supply chain to capture their perspectives on how a software bill of materials, or “SBOM,” is helping them today, and what they could do in the future if this practice became more widespread. We are working toward a shared vision of what the “minimum viable” implementation looks like, and how it can be implemented across the supply chain. Several health care participants have demonstrated the value of SBOM through a proof of concept, by sharing data between a handful of large medical device manufacturers (Siemens, GE, Philips) and hospitals (Mayo Clinic, NY Presbyterian, Cedars-Sinai).

Conclusion

Over the past three decades, the Internet has been transformational for the American economy. According to the Bureau of Economic Analysis, the digital economy represented nearly 6.5 percent of the nation’s GDP, or $1.2 trillion in 2016. America’s established leadership in technology has resulted in millions of jobs and remarkable prosperity, and it also means that Americans rely on the Internet in their daily lives more than ever. Because of this, we must work harder than ever to ensure that the infrastructure supporting the Internet is secure.

NTIA is committed to coordinating across the Federal Government and engaging with the private sector to create a more secure Internet infrastructure. Security is the first step to ensuring that the United States can continue to harness the economic benefits of this vital part of the economy for American businesses and American workers as new technologies, including 5G, become integrated into our daily lives.

Thank you for the opportunity to participate in this hearing. I look forward to your questions.

Diane Rinaldo
Assistant Secretary, National Telecommunications and Information Administration,
Department of Commerce (Acting)

Diane Rinaldo was sworn in as Deputy Assistant Secretary for Communications and Information at the Department of Commerce on April 20, 2018. On May 9, 2019, she became Acting Assistant Secretary for Communications and Information for the Department, and Administrator of the National Telecommunications and Information Administration, the Executive Branch agency principally responsible for advising the President on telecommunications and information policy.

Focusing on cybersecurity and technology policy, Diane has extensive experience in government and the private sector throughout her career. She staffed the House Permanent Select Committee on Intelligence, where she was the lead committee staffer on Congress' landmark cybersecurity legislation, the Cybersecurity Act of 2015. She also served as the oversight and budget monitor for the National Security Agency and the defense network systems, and served as Deputy Chief of Staff to Congressman Mike Rogers as his top technology policy staffer.

Recognized for her work on cybersecurity, Rinaldo was awarded the Executive Women's Forum's 2016 Influencer of the Year award. She earned a bachelor's degree in Political Science from the University of Maine and an Executive Certificate from the Kennedy School of Government at Harvard University for cyber studies.

STATEMENT OF

MR. B. EDWIN WILSON

DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR

CYBER POLICY

TESTIMONY BEFORE THE HOUSE ARMED SERVICES

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING

THREATS AND CAPABILITIES AND THE HOUSE OVERSIGHT

AND REFORM SUBCOMMITTEE ON NATIONAL SECURITY

SEPTEMBER 10, 2019

INTRODUCTION

Chairman Langevin, Chairman Lynch, Ranking Member Stefanik and Ranking Member Hice, and members of the committees, thank you for the opportunity to testify on the role of the Department of Defense (DoD), in partnership with other Federal departments and agencies, in securing the Nation's internet architecture.

I would first like to thank Congress for its broad and continued support of the Department's cyber missions, including the enactment of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019, which supports a range of military operations in cyberspace to deter, disrupt, and defeat, malicious cyber activities, as well as our constructive, ongoing dialogue with the House and Senate Armed Services Committees regarding the development of the NDAA for Fiscal Year 2020.

THE THREAT

To begin, I would like to offer a perspective on the cyber threat environment. As the 2018 National Defense Strategy and the 2018 DoD Cyber Strategy make clear, the U.S. homeland is no longer a sanctuary from cyber threats. The United States' strategic competitors are conducting cyber-enabled campaigns to erode U.S. military advantages, threaten our Nation's critical infrastructure, and compete using predatory, non-free market economic practices to undermine our prosperity.

In particular, we are engaged in long-term power competition with China and Russia. As part of this long-term power competition, these States are engaged in persistent campaigns against the United States in and through cyberspace. These campaigns are conducted below the threshold of armed conflict but collectively pose long-term strategic risk to the Nation, our allies, and our partners. Our strategic posture acknowledges the growing risk to our military advantage and to the Nation if we do not deter, disrupt, and defeat these threats. The Department, working alongside our U.S. Government partners, continues to strengthen public and private partnerships in order to mitigate emerging cyber threats, but more must be done and will be done.

STRATEGIC POSTURE

In September 2018, the President released the National Cyber Strategy, which highlights the growing threat that malicious cyber actors pose to our national security. The 2018 DoD Cyber Strategy prioritizes the challenge of Great Power competition and recognizes that the Department must adopt a forward-leaning posture to compete with, and counter, determined and rapidly maturing adversaries. The strategy normalizes the Department's efforts in the cyberspace domain, integrating cyberspace operations into military operations in the physical domains of air, land, sea, and space.

The DoD Cyber Strategy also makes clear that the Department's focus in cyherspace, like in other domains, is to "defend forward"—that is, to prevent or mitigate threats before they harm U.S. national interests. We defend forward by conducting operations that range from collecting information to gain insight about hostile cyber actors and their intent, to exposing malicious cyber activities and associated infrastructure publicly, to disrupting malicious cyber activities directly. Through a persistent day-to-day presence in cyberspace, we can best monitor our adversaries and develop an effective national cyber defense. This approach simultaneously imposes costs on adversary malicious actors and enables our interagency, industry, and international partners to strengthen their resilience, close vulnerabilities, and defend critical networks and systems.

In parallel with defending forward, the Department is continually working with its partners to strengthen the resilience of networks and systems that contribute to current and future U.S. military advantages. The Department has previously focused its defensive efforts on military platforms and systems and networks owned and operated by DoD. However, the evolving cyber threat and increasingly provocative activities of key competitors have demonstrated vulnerabilities that extend beyond the DoD Information Network. The vulnerability of U.S. critical infrastructure to cyberattacks means that adversaries could disrupt military command and control, banking and financial operations, the transportation sector, the energy sector, and various means of communication. As a result, supporting U.S. Government efforts in securing and defending the Nation's critical infrastructure is also a priority under the DoD Cyber Strategy.

Our interagency, international, and private sector partners are key to ensuring that DoD can operate and project power in a contested cyber environment. Empowered by the 2018 DoD Cyber Strategy, DoD's role in defending the homeland is focused outward and supports our interagency partners, including the Department of Homeland Security (DHS), represented here this afternoon by Assistant Director Manfra. Supporting U.S. Government efforts to secure and defend U.S. critical infrastructure has become an enduring DoD activity, as demonstrated in the successful whole-of-government effort to secure the 2018 U.S. midterm elections.

CHALLENGES TO SECURING THE NATION'S INTERNET ARCHITECTURE

It has become increasingly clear, as the National Security Strategy released in December 2017 identified and as President Trump has noted, that "economic security is national security." A strong, defensible cyber infrastructure fosters economic growth, protects our liberties, and advances our national security. As the U.S. military becomes more and more technologically advanced, our demand for connectivity that's always-on and always available will only increase. DoD relies heavily upon the global internet architecture including internet exchange points, data centers, content delivery networks, undersea cables, international telecommunications, and related infrastructure. Undersea cable systems are vital to the execution of DoD's missions globally. The Department has been leasing bandwidth on privately-owned undersea cable systems since the 1980s. DoD prioritizes mission-essential traffic and the Defense Information Systems Agency (DISA) is constantly working with the Combatant Commands, Military Departments, and Defense Agencies to meet mission requirements.

The U.S. Government has a limited and specific role to play in defending against attacks on our Nation's internet architecture, including through DoD's trusted relationships with industry. Security was not a major consideration when the Internet was designed and fielded. Although computers and network technologies underpin U.S. military warfighting superiority by enabling the Joint Force to gain the information advantage, strike at long distance, and exercise global command and control, the private sector owns and operates well over ninety percent of all of the interdependent networks of information technology infrastructures across the cyber domain. At the same time, the Nation's telecommunications infrastructure is primarily owned by commercial entities. Our adversaries target our Nation's weakest links, and vulnerabilities are consistently found across the full scope of the

Internet ecosystem be it government or industry targets.

The Department, which views the challenges it faces in performance of its critical missions principally through a national security lens is nonetheless highly dependent on privately-owned infrastructure, decisions concerning which are regularly guided by ordinary business – or economic – considerations. Recognizing this inherent tension, defending national critical infrastructure, including the Nation's internet architecture, from significant foreign malicious cyber activity has become an area of increased emphasis for the Department.

Any large-scale disruption or degradation of national critical infrastructure would constitute a national security concern, as would threats to DoD critical technology information (CTI) and other controlled unclassified information (CUI) processed or stored on non-DoD-owned systems and networks, demanding close cooperation and strong relationships with the private sector. This priority is formalized in the DoD Cyber Strategy's directive that the Department be prepared to defend assertively non-DoD-owned Defense Critical Infrastructure – referring to the composite of DoD and non-DoD assets essential to develop, project, support, and sustain military forces and operations worldwide. Presidential Policy Directive-21, "Critical Infrastructure Security and Resilience," prescribes that DoD is the Sector Specific Agency (SSA) for the DIB critical infrastructure sector. As the Federal lead of the DIB critical infrastructure sector, DoD and DIB partners work together to improve security and resilience of DIB networks and systems, working closely with DHS and other partners.

The Department's cybersecurity initiatives are an important aspect of the overall and ongoing efforts to deny, disrupt, and neutralize critical technology transfer to China. In October 2018, the Secretary of Defense established the Protecting Critical Technology Task Force (PCTTF) to align the Department's efforts to protect its critical technologies and address broader systematic issues. Through the work of this Task Force, the Department is driving protection efforts towards its most critical technologies, elevating security across our Research, Development, and Acquisition communities, and organizing the Department's operational response as warranted. In addition, under Executive Order 13873, Securing the Information and Communications Technology and Service Supply Chain, DoD will work with the Department of Commerce to limit foreign adversaries' ability to create and exploit vulnerabilities in our national information and communications technology in order to commit malicious cyber-enabled actions against US critical cyber infrastructure.

DoD is focused on how to improve collaboration with industry and other Federal departments and agencies, including DHS, the Federal lead for improving the security and resilience of much of the Nation's critical infrastructure and SSA for telecommunications. Our partnership with industry includes cyber threat information sharing and collaboration to better protect DoD information as well as industry intellectual property. It will take a whole-of-society partnership to defend our vital interests successfully in an era of intensifying adversarial competition.

COLLABORATING WITH INTERAGENCY AND INDUSTRY PARTNERS

In support of one of the Department's most critical interagency partnerships, DoD and DHS have worked together to establish a framework to drive domestic preparedness and critical infrastructure efforts. In October 2018, then-Secretary of Defense Mattis and then-Secretary of Homeland Security Nielsen signed a joint memorandum that frames how DHS and DoD will secure and defend the homeland from cyber threats. The memorandum makes clear that DHS's mission to protect critical infrastructure and DoD's mission to defend the homeland by defending forward are mutually reinforcing. DoD and DHS each derive unique insights from our daily activities – whether from DoD's intelligence collection and cyber operations, or from DHS's cyber operations to protect Federal networks and critical infrastructure in partnership with the private sector – that inform our respective missions.

Implementation of the joint memorandum is underway. A Joint DoD-DHS Cyber Protection and Defense Steering Group Charter was signed in November 2018, and the Steering Group leadership has directed the prioritization of cyber security cooperation between our departments and meets regularly to assess our progress.

DoD and DHS worked together to ensure that all appropriate Federal Government tools and resources were available to protect and defend the 2018 U.S. midterm elections from foreign interference. As part of this effort, DoD regularly shared information with DHS and the Federal Bureau of Investigation (FBI). It also provided standing approval for DoD personnel to support DHS cyber incident response activities in the event of a significant cyber incident impacting elections infrastructure. DoD dispatched an advance team to DHS's National Cybersecurity and Communications Integration Center to improve situational awareness, communication, and team integration for better unity of effort if DHS requested DoD assistance.

Beyond elections, the Department works closely with DHS, FBI, and stakeholders from across the Federal Government, the private sector, and international partners concerning risks to critical infrastructure, including telecommunications networks. Through a series of Pathfinder initiatives, DoD is focused on improving its collaboration with DHS and other SSAs in support of their missions to assist the private sector – including select critical infrastructure partners – by sharing threat information, conducting collaborative analysis of vulnerabilities and threats, and mitigating those risks.

Whole-of-nation collaboration is crucial to our ability to build resilience and deter or defeat strategic threats to U.S. national interests and infrastructure. Although the Department supports DHS's efforts to enable private sector entities to defend their networks, these Pathfinders in turn enable DoD to partner with DHS to leverage private sector threat information to inform DoD cyberspace operations.

CONCLUSION

Thank you again for the opportunity to appear before you today. With the 2018 National and DoD Cyber Strategies in place, the Department has the right policy and guidance to support the defense of our Nation in cyberspace. The Department has undertaken extensive work with DHS and other SSAs to improve our collective defense of the homeland and the Nation's internet architecture. That said, there is much left to do. I look forward to working with Congress as we address these challenges, and I welcome your questions.

B. Edwin Wilson
Deputy Assistant Secretary of Defense for Cyber Policy

Mr. B. Edwin Wilson was appointed the Deputy Assistant Secretary of Defense for Cyber Policy on 20 February 2018. In this capacity, he supports the Secretary of Defense and other senior Department of Defense leaders by formulating, recommending, integrating, and implementing policies and strategies to improve DoD's ability to operate in cyberspace.

Mr. Wilson retired from the U.S. Air Force after serving on active duty for over thirty-two years. In his last duty assignment, Major General (retired) Wilson served as the Deputy Principal Cyber Advisor to the Secretary of Defense and Senior Military Advisor for Cyber, Office of the Under Secretary of Defense for Policy, Office of the Secretary of Defense, the Pentagon, Washington, D.C. In these capacities, General Wilson supported the Principal Cyber Advisor as the primary advisor to integrate and oversee the development of all DoD cyber capabilities, activities and policy, as well as provided senior military perspective on cyber policies, strategies and plans to guide DoD efforts in cyberspace.

Prior to this duty, General Wilson was triple-hatted serving as the Commander, 24th Air Force; Commander, Air Forces Cyber; and Commander, Joint Force Headquarters-Cyber at Joint Base San Antonio-Lackland, Texas.

General Wilson also served in various assignments, including space and cyberspace operations, planning, strategy, policy, acquisition and combat support. The general commanded at the squadron, group, wing and numbered Air Force levels, as well as served on the staffs of Headquarters Air Force, Air Force Space Command, 24th Air Force, the National Reconnaissance Office, North American Aerospace Defense Command and the former U.S. Space Command.

Mr. Wilson received his Bachelor of Science degree in Electrical Engineering from the U.S. Air Force Academy; a Master of Science degree in Electrical/Computer Engineering from Northeastern University; and a Master of A the U.S. Air Force's School of Advanced Airpower Studies.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

SEPTEMBER 10, 2019

RESPONSE TO QUESTION SUBMITTED BY MR. WALTZ

Ms. MANFRA. The majority of submarine cables are privately owned by a mix of domestic and foreign entities. The protection of these cables is a complex question, considering they travel through domestic and international waters, some of which are contested areas. While the U.S. and its allies have significant interest in ensuring the safety and continued functionality of submarine cables, it will require a "concerted effort" from the United States and its allies to ensure the confidentiality, integrity, and availability of the data that traverses subsea systems, in addition to the physical security of the cable and cable landing station. While DHS is the communications sector-specific agency per PPD–21, the current responsibility for defending undersea cables landing in the United States involves a "whole of government" approach, which includes the Navy in our Exclusive Economic Zone (EEZ) and the Coast Guard within our 12 mile nautical sovereignty zone. Team Telecom—primarily made up of executive branch agencies DOD, DHS, and DOJ—acts as an advisory committee to the FCC in matters related to foreign investment into US domestic communications infrastructure. Letters of Assurance (LOAs) and Network Security Agreements (NSAs) are memorandums of understanding between the USG and the cable owners/operators that govern the location of assets, types of principal equipment, physical access controls, and other relevant factors surrounding the functionality and protection of undersea cable systems. DOD, DHS, and DOJ enforce Team Telecom agreements through periodic compliance and mitigation visits to cable landing sites, network operations centers, and other relevant infrastructure. The Department of Justice and Federal Bureau of Investigation investigate and prosecute criminal acts and espionage-related activities. These activities are informed by reporting from the intelligence community and various other federal agencies. [See page 30.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

SEPTEMBER 10, 2019

QUESTIONS SUBMITTED BY MS. STEFANIK

Ms. STEFANIK. As you think about our vulnerabilities, are insider threats an area of concern with respect to our Nation's internet architecture, from either within government or even industry and the private sector? How do you monitor for insider threats? Are there policies in place that allow you to have a dialogue and understand insider threats from within industry and the private sector, or is this difficult given privacy issues?

Ms. MANFRA. Malicious insiders pose a serious threat to organizations in the public and private sectors, including those that own, operate and support our internet architecture. Insiders' authorized access and detailed knowledge of critical assets offers them opportunities to compromise information, sabotage infrastructure, or inflict harm upon co-workers. While insider-threats will always remain a concern, it is possible to significantly limit the amount of damage a bad insider can do by properly implementing hardware, software, and procedural controls to sensitive networks To help counter this threat, the Cybersecurity and Infrastructure Security Agency (CISA) strongly advocates for an engaged workforce, one that is trained to recognize and report suspicious behavior or activity and can help defend against insider threats. Personnel security, as well as technical and procedural countermeasures, can also assist in detecting suspicious behavior and minimizing the risk that insider threats present. In addition to free educational materials, CISA's Protective Security Advisors work with organizations throughout the U.S. to learn how they are prepared to deal with insider threats, and to help organizations develop capabilities to mitigate potential insider threats through in-person training workshops. Voluntary information sharing and collaboration with industry and private-sector organizations on the value of insider threat programs and mitigation techniques has been a valuable tool in CISA's infrastructure security and cybersecurity missions.

Ms. STEFANIK. Given the private sector and industry own the overwhelming majority of communications infrastructure, how do you engage on a recurring basis with the private sector, especially major carriers and telecommunications companies? What are the recurring themes in these conversations? Are there policy differences, or specific problems you are currently working through?

Ms. MANFRA. Information and Communication Technology (ICT) Supply Chain Risk Management Task Force

- The Communications Sector co-chairs the ICT Supply Chain Risk Management Task Force (Task Force).
- The Task Force was formed in 2018, with strategic mandates to provide a forum for the collaboration of private sector owners and operators of ICT critical infrastructure and to provide advice and recommendations to the U.S. Department of Homeland Security (DHS) on means for assessing and managing risks associated with the ICT supply chain.
- The working groups have developed policy recommendations and guidance documents for the Federal Acquisition Security Council's consideration. The Task Force has produced an Interim Report on its activities for the first year and will begin its year-two activities in the fall of 2019. National Critical Functions
- DHS, through the CISA National Risk Management Center (NRMC), released a set of National Critical Functions in April 2019. The Communications Sector actively participated in this work effort and will continue to be a key partner as CISA begins to build a risk register that will add a more prioritized and strategic overlay to CISA's critical infrastructure protection efforts.

Tri-Sector Executive Working Group

- Actively participates as a member of this Critical Infrastructure Partnership Advisory Council Working Group that was established by the NRMC to collaborate, to understand, prioritize, and manage systemic risk, and plan for and respond to cross sector incidents. Specifically, the Communications Sector, along with the Financial Services Sector and Electricity Sub-sector worked together to (1) better understand systemic risk that might impact all three sectors; (2) build cross-sector incident response playbooks; and (3) direct the development of better intelligence collection requirements to these sectors.

National Security Telecommunications Advisory Committee

- The President's National Security Telecommunications Advisory Committee (NSTAC) provides industry-based analysis and recommendations to the President and the Executive Branch regarding a wide range of policy and technical issues related to telecommunications, information systems, information assurance, infrastructure protection, and other national security and emergency preparedness (NS/EP) concerns.
- President Ronald Reagan created the NSTAC when he signed Executive Order (EO) 12382, President's National Security Telecommunications Advisory Committee. The NSTAC is composed of up to 30 Presidentially-appointed senior executives, who represent various elements of the telecommunications and information technology industries. The NSTAC meets quarterly to report its activities, while providing recommendations to the President on policy and enhancements to NS/EP telecommunications.
- The NSTAC recently completed a study of the technology capabilities critical to NS/EP functions in the evolving ICT ecosystem. The goal was to determine what Government measures and policy actions could be taken to manage near-term risks, support innovation, and enhance vendor diversity in this industry. Specifically, the NSTAC analyzed threats to supply chain security and resiliency that exist due to the diminishing number of trusted manufacturers producing ICT components.
- In September 2019, the NSTAC submitted its recommendations in the NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem. In the report, the NSTAC recommended that the President create a new role within the White House called the Senior Advisor to the President for ICT Resiliency; and develop a national strategy on advancing resiliency and fostering innovation in the ICT ecosystem, empowering whole-of-nation resources to pursue a more fundamentally safe internet environment for critical services.
- On October 17, 2019, the NSTAC kicked off its next study, examining the importance of software-defined networking (SDN). This study will examine the importance of SDN; identify the challenges and opportunities related to SDN; and assess the utilization of SDN and corresponding mitigation issues. The goal of the study is for the NSTAC to (1) develop a strategic plan and best practices for deploying SDN in Federal networks and critical infrastructure; and (2) provide the Government with a better understanding of how SDN can potentially address security challenges including ICT supply chain risks.

Network Security Information Exchange

- The Network Security Information Exchange (NSIE) is an information sharing forum charged with devising strategies for mitigating cyber threats to the Public Network (PN). The NSIE's primary objective is to enhance the security of communications networks required for NS/EP.
- CISA participates in bi-monthly joint NSIE meetings, which include membership across U.S. Government and industry. NSIE membership also includes industry and Government participation from the Five Eyes. Industry participation includes major carriers and telecommunications companies (i.e., NSTAC NSIE members, including AT&T, Verizon, etc.). CISA provides NSIE leadership in the form of the U.S. Government NSIE chair and program manager.
- Joint NSIE meetings include a closed session, where NSIE members share information on emerging network security challenges, vulnerabilities, and mitigation strategies.
- The NSIE periodically assesses risks to the PN from electronic intrusions. In December 2014, the NSIE completed An Assessment of the Risk to the Cybersecurity of the Public Network, which focused on how changes in technology have affected the PN and recommended effective mitigation strategies. NSIE members plan to update the risk assessment in 2020, and may examine new issues such as DNS encryption, log management, workforce training, 5G, and insider threat. CISA will support development of the document.

National Security and Emergency Preparedness (NS/EP) Communications

- The Department maintains a unique contractual relationship with the private sector, through major carriers and telecommunications companies to fulfill responsibilities of EO 13618, Assignment of National Security and Emergency Preparedness Communications Functions.
- CISA's Emergency Communications Division conducts a bi-monthly Service Provider Council forum to address nonproprietary telecommunications service matters dealing with NS/EP Communications requirements for priority service ca-

pabilities within the carrier networks as they upgrade switching technologies to all internet protocol based.

Ms. STEFANIK. With regard to emerging technologies, specifically 5G technology, and the exponential increase in the number of connected devices and services in the very near future, how exactly are you factoring this technological evolution into your strategies and your coordination with the private sector, to fully understand the impacts and risks?

Are there any policy limitations or laws limiting your approach? How about the challenges with spectrum, the limited availability, and the potential for dynamic spectrum sharing technologies to help manage the on-ramp of things such as 5G?

Ms. RINALDO. The National Telecommunications and Information Administration (NTIA) is taking a multifaceted approach to address the challenges of the proliferation of 5G. This starts with assessing how such technologies will alter the communications marketplace and the impact they will have on numerous adjacent industries and applications. Consistent with the Administration's view that the private sector must lead in 5G development and deployment, NTIA works to support U.S. technological leadership by making sufficient spectrum available, facilitating broadband deployment, ensuring U.S. networks are secure, supporting industry in global technology standards development, and promoting needed research, development, testing and evaluation efforts. Access to spectrum is critical to 5G. Although spectrum is a limited resource, NTIA has been very successful in its continuing collaboration with the Federal Communications Commission to make additional spectrum bands available for commercial use while ensuring federal agencies have the spectrum needed to perform their important missions. In some instances, exclusive-use licenses are made available but, because of the congested nature of the spectrum environment, increasingly most spectrum bands are shared, including between federal government and non-federal government users. Traditional, static methods of sharing, principally by excluding new entrants from using specific frequencies or from operating in specific geographic areas, are starting to be replaced by more dynamic sharing models, such as the newly launched Citizens Broadband Radio Service (CBRS) 3.5 GHz band. CBRS represents a significant advance in dynamic spectrum sharing and may prove applicable to future spectrum management frameworks.

Ms. STEFANIK. As you think about our vulnerabilities, are insider threats an area of concern with respect to our Nation's internet architecture, from either within government or even industry and the private sector? How do you monitor for insider threats? Are there policies in place that allow you to have a dialogue and understand insider threats from within industry and the private sector, or is this difficult given privacy issues?

Ms. RINALDO. Every organization faces internal threats, including Internet infrastructure organizations. Identifying and responding to these threats requires careful risk management practices, which can include practices ranging from controlling use of administrative privileges, to data loss and theft prevention, to physical security of key assets. A number of resources exist to help organizations assess insider risks and develop an insider threat program, including those published by the Cybersecurity and Infrastructure Security Agency, the National Institute for Standards and Technology, and the SANS Institute. For its part, NTIA participates in interagency discussions with our federal partners, and works through a range of industry fora to help the private sector better address their cybersecurity risks, including insider threats.

Ms. STEFANIK. Given the private sector and industry own the overwhelming majority of communications infrastructure, how do you engage on a recurring basis with the private sector, especially major carriers and telecommunications companies? What are the recurring themes in these conversations? Are there policy differences, or specific problems you are currently working through?

Ms. RINALDO. NTIA engages with the private sector, including major carriers and telecommunications companies, in multiple ways. For example, NTIA is an active participant in the Government Coordinating Councils (GCC) for the Communications (CGCC) and Information Technology (ITGCC) sectors, and regularly attends both the "joint" and "quad" meetings with private sector participants. These Department of Homeland Security and Sector-Specific Agency-led councils provide a useful forum for bringing together government and private sector organizations. NTIA has established its leading role in cybersecurity through use of the multistakeholder process to convene stakeholders to address pressing cybersecurity concerns. These efforts have broad participation from industry, academia, research institutions, and federal departments and agencies. Our multistakeholder process efforts have addressed a wide range of topics, including software component transparency, Internet of Things (IOT) component upgrades and software patching, and coordinated vulnerability disclosure. NTIA's current multistakeholder process brings stakeholders who draft documents that are approved by a consensus of the stakeholders on how to develop a "software bill of materials" that list the components that make up software—a concept similar to a food ingredients list for products on grocery store shelves. The goal of the multistakeholder process is to increase transparency around the use of third-party software components so that when vulnerabilities are detected, there is a way to quickly respond to and recover from risks.

Ms. STEFANIK. As you think about our vulnerabilities, are insider threats an area of concern with respect to our Nation's internet architecture, from either within government or even industry and the private sector? How do you monitor for insider threats? Are there policies in place that allow you to have a dialogue and understand insider threats from within industry and the private sector, or is this difficult given privacy issues?

Given DOD's connections to the Defense Industrial Base, what unique responsibilities does the Department have as the lead for the DIB as a critical sector?

Mr. WILSON. Insider threats to the Department, the Defense Industrial Base (DIB), and Defense Critical Infrastructure are of great concern to the Department. The Office of the Under Secretary of Defense for Intelligence (USDI) is the overall lead for countering insider threats in DOD. As the Sector Specific Agency (SSA) for the DIB, DOD facilitates its DIB partners' efforts to improve the security and resilience of DIB networks and systems, in close coordination with the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and others. In addition, USDI and the Office of the Chief Information Officer (CIO) have forged a partnership to secure networks within the perimeter to monitor for potential insider threats. The National Industrial Security Program (NISP) is administered by the Defense Counterintelligence and Security Agency (DCSA) on behalf of the Department of Defense and 33 other Federal departments and agencies. Under the NISP, cleared industrial facilities are required to have an insider threat program consistent with E.O. 13587 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. The intent is to ensure that insider threat programs at commercial facilities are organized and run like those found at Executive Branch departments and agencies. Many of the major defense contractors have established corporate insider threat programs. The Department remains committed to enabling robust security practices beyond cleared facilities in partnership with the private sector. Recently, both the White House Office of Science and Technology Policy (OSTP) and the Under Secretary of Defense for Research and Engineering sent letters to the U.S. research community to increase awareness of insider threats like foreign talent programs that seek to undermine, exploit, and erode our world class research enterprise. DOD shares insider threat related data with industry partners, as permitted by law. Through a series of pathfinder initiatives, the Department is focused on improving its collaboration with DHS, other SSAs, and appropriate private sector entities—including select critical infrastructure partners—by sharing threat information, conducting collaborative analysis of vulnerabilities and threats, and, when authorized, mitigating those risks. These pathfinders, in turn, enable the Department and its Federal partners to leverage private sector threat information to support DOD's mission.

Ms. STEFANIK. Given the private sector and industry own the overwhelming majority of communications infrastructure, how do you engage on a recurring basis with the private sector, especially major carriers and telecommunications companies? What are the recurring themes in these conversations? Are there policy differences, or specific problems you are currently working through?

Who specifically in the Department of Defense does this outreach and maintains awareness?

Mr. WILSON. DHS serves as the SSA for the Communications and Information Technology Sectors, and works closely with DOD, the Department of Justice (DOJ), the Department of Commerce, the Federal Communications Commission (FCC), the General Services Administration, the Intelligence Community, and the private sector to address both short-term and longer-term challenges regarding risks to telecommunications networks. Within DOD, the Office of the Chief Information Officer is the lead for the Department's participation on Team Telecom, an interagency working group of representatives from Federal government entities, including the DHS and DOJ co-chairs, charged with ensuring the national security of our telecommunications networks and infrastructure. Team Telecom is involved in reviewing foreign acquisitions of U.S. communications infrastructure as well as evaluating FCC Section 214 license applications to operate or provide telecommunications networks in the United States for national security, public safety, and law enforcement concerns.

QUESTIONS SUBMITTED BY MR. KIM

Mr. KIM. There was mention of individual agency exercises, but what about real-world exercises between different agencies? Who do you think should be invited to these exercises? And what are the roles for private companies and State and local governments? And who should be in charge of running these?

Ms. MANFRA. CISA conducts exercises with agencies to help increase cybersecurity preparedness and resilience. Some exercises are internal to a single agency, while others include multiple agencies or even private sector partners. One noteworthy effort is Cyber Storm, CISA's biannual capstone cyber exercise. This includes multiple federal agencies, as well as state and international governments, and the private sector. The exercise engages players in the discovery of and response to a widespread cyber incident. Agencies walk through their plans and procedures to share information, coordinate with partners, and simulate response actions. Currently, approximately 150 organizations are slated to participate in Cyber Storm 2020. Participants vary, based on the specific goal and objectives of the exercise. CISA usually recommends a cross-section of people who have a role in cybersecurity. This can include senior leadership, cybersecurity or information technology (IT) security staff, incident response teams, analysts, legal, public affairs, human resources (HR), or the data or system owners. Private companies and state and local governments often participate in exercises as players. Cyber Storm is one example of an exercise that engages all stakeholders in one coordinated effort. CISA also conducts exercises for major events like the Super Bowl, which bring together government and private sector to talk about how they would share information or respond to a cyber incident that would have impacts across their organizations. CISA is well-positioned to run these types of exercises for various reasons. First, we have responsibilities for federal cybersecurity and asset response, so the exercises outputs inform potential plans and procedures and help educate people on CISA's role. Second, CISA has existing relationships across federal agencies, state and local governments, and the private sector, which enables us to engage a wide swath of stakeholders in exercises. Finally, CISA has analysts and subject matter experts looking at cyber threats daily, who can feed that information into exercises to ensure they address current and realistic threats and vulnerabilities.

Mr. KIM. There was mention of individual agency exercises, but what about real-world exercises between different agencies? Who do you think should be invited to these exercises? And what are the roles for private companies and State and local governments? And who should be in charge of running these?

Ms. RINALDO. The Department of Commerce is a member of the Federal Emergency Management Agency's (FEMA) Exercise Implementation Committee and the National Security Council's (NSC) Exercise and Evaluation Sub-Policy Coordinating Committee. NTIA participates in national level exercises, coordinated among Commerce agencies at the Department level. NTIA's level of participation is determined by the specifics of the exercise and its relevance to NTIA's statutory responsibilities. For example, NTIA participates in the Eagle Horizon and CyberStorm exercises. Eagle Horizon is the mandatory, annual, integrated continuity exercise for all federal executive branch departments and agencies, as required by National Continuity Policy. CyberStorm is the Department of Homeland Security's biennial exercise series to strengthen cyber preparedness in the public and private sectors. The Department also coordinates participation in senior official exercises directed by the NSC. These exercises are held at the Assistant Secretary through Secretary level. In addition to NTIA's direct participation in national-level exercises, members of the First Responder Network Authority (FirstNet Authority) and FirstNet personnel from AT&T have engaged with state, local, and tribal entities through demonstrations and independent exercise activities. Typically, FirstNet will collaborate with a state or local entity to conduct the exercise. This summer, FirstNet participated in FEMA's Shaken Fury exercise near Memphis, Tennessee, involving a series of tabletop, functional, and full-scale exercises in partnership with the U.S. Department of Energy, U.S. Northern Command, state and local governments, and the private sector.

Mr. KIM. There was mention of individual agency exercises, but what about real-world exercises between different agencies? Who do you think should be invited to these exercises? And what are the roles for private companies and State and local governments? And who should be in charge of running these?

Mr. WILSON. The Federal Emergency Management Agency (FEMA) is the lead for the National Exercise Program (NEP), which addresses National response across Federal, State, and local levels, and includes non-governmental organization, private sector, and private citizen participation, depending on the scenario. NEP exercises are mandatory for Executive Branch departments and agencies and are used to address multi-agency coordination in the performance of National Essential Functions. For example, in 2020, DOD will participate in the FEMA-led National Level Exercise, which is focused on domestic cyber incidents and is intended to link together a broad range of interagency exercises around a common theme. Additionally, each Federal department and agency hosts exercises to inform their respective missions, learn lessons, and improve mission readiness. The goals and objectives of an exercise drive the scope, scenarios, and participation. Although some exercises are internally focused on an individual department or agency, others include broad interagency and other participation. DOD hosts a range of internal and interagency exercises, and supports and participates in exercises hosted by DHS, the Department of Energy, the Intelligence Community, and others. In August 2019, DOD hosted a table-top exercise to improve DOD's ability to provide Defense Support of Civil Authorities (DSCA) in response to a cyber incident. The exercise included representatives from DOD, other Federal departments and agencies, the energy sector, and State and local governments. U.S. Northern Command (USNORTHCOM) hosted a table-top exercise in October 2019 focused on improving DOD's operational coordination structure for DSCA responses to cyber incidents, with the goal of improving and streamlining interagency integration in advance of a cyber incident. U.S. Cyber Command (USCYBERCOM) hosts the annual CYBER GUARD exercise, which focuses on refining DOD's readiness to respond to a domestic cyber incident. CYBER GUARD includes a wide range of participants from Federal departments and agencies and other entities.

QUESTIONS SUBMITTED BY MS. HOULAHAN

Ms. HOULAHAN. I also serve on the Foreign Affairs Committee. I am curious what collaboration has looked like and will look like for each of your respective agencies as the Department of State stands up the Bureau of Cyberspace Security and Emerging Technologies and as other agencies consider creating similar teams? Further, do you see a need for the Presidential Policy Directive 21 (PPD–21), which divvies up responsibilities within the Federal Government for cyber, to be updated to reflect the emergence of these new departments?

Ms. MANFRA. DHS collaborates and coordinates on international cyber engagements with the U.S. Departments of State, Defense, Justice, Commerce, and other federal agencies. At present, CISA and the U.S. Department of State's Office of the Coordinator for Cyber Issues collaborate on a range of issues from cyber capacity building and critical infrastructure protection, to cybersecurity awareness. As State stands up the Bureau of Cyberspace Security and Emerging Technologies, DHS expects coordination to increase and for additional partnership with international counterparts on cybersecurity. This new office at State will help enhance the outreach to international partners and be in direct support of what is already stated in Presidential Policy Directive 21 (PPD–21), which currently provides that "the Department of State, in coordination with DHS, Sector Specific Agencies, and other Federal departments and agencies, shall engage foreign governments and international organizations to strengthen the security and resilience of critical infrastructure located outside of the United States and to facilitate the overall exchange of best practices and lessons learned for promoting the security and resilience of critical infrastructure on which the Nation depends." As PPD–21 already provides for this role for the State Department, CISA does not see the need to update PPD–21.

Ms. HOULAHAN. I often ask our witnesses to speak on two workforce challenges facing our government, as well as our society. First, do you feel your organization has the necessary expertise to execute your mission? Is our workforce being adequately prepared to meet these emerging threats? Do you have any concerns that this pipeline is lacking? Finally, what sorts of challenges does your organization face when recruiting technical experts when competing with the private sector? What could we do to support these recruitment efforts?

Ms. MANFRA. 1. The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure, potentially placing the Nation's security, economy, and public safety and health at risk. Paramount to equipping the Federal Government and the nation's critical infrastructure entities with cybersecurity information and assistance is a workforce with the right competencies, knowledge, skills, and abilities to underpin CISA's mission capabilities, in support of the National Cybersecurity Strategy and Risk Management Framework. CISA recruits and builds these competencies through buying, building, and borrowing talent. CISA focuses on hiring the best and brightest talent and augments its capability through contractors. Training is paramount to mission success and CISA continues to cultivate and capitalize on opportunities to invest in its employees and equip them with maturation of current skills, as well as expand upon them. While CISA employs superior talent, expertise is not a static endeavor; but rather, a continuous effort. Through training, CISA strives to prepare a cybersecurity workforce with the skills to be more resilient and excel at mission capability requirements.

2. The President's Management Agenda laid out a long-term vision for modernizing the Federal Government's key areas that will improve the ability deliver mission outcomes. To drive the management priorities, the Administration created Cross-Agency Priority (CAP) Goals, centered on "Modernizing Government for the 21st century." One of the three CAP Goals calls for investing in people and creating the "Workforce for the 21st Century." This theme is carried throughout the National Cybersecurity Strategy and the DHS Cybersecurity Strategy, calling for the use of innovative solutions to "keep pace with the current pace of change." The systematic approach to meet CISA's workforce needs incorporates the concepts of buying, building, and borrowing talent. DHS has largely been focused on buying talent through the existing hiring system and the future enhanced Cyber Talent Management System. The DHS Office of the Chief Human Capital Officer (OCHCO) is leading the effort to prepare for the launch of the CTMS and create the DHS Cybersecurity Excepted Service. The effort will modernize talent management to align to and keep pace with the cybersecurity work of the Department by taking a comprehensive approach to recruit and retain talent modeled after industry best practices. Competition in the marketplace to recruit and retain cyber professionals continues to grow, along with the demand for cyber defense experts to protect our nation's networks and information systems. To overcome these challenges, the Administration has focused on efforts under the Federal CAP Goal, Developing a Workforce for the 21st Century, to improve service to America through enhanced alignment and strategic management of the Federal workforce. To further build upon the work already done and increase employee engagement, on May 2, 2019, the Administration published the Executive Order on America's Cybersecurity Workforce, with the direction to strengthen the cybersecurity capability of the Federal workforce through increased integration and skills enhancement opportunities under a rotational program. The Federal Cybersecurity Rotation Program is a career broadening opportunity for cybersecurity practitioners to expand their cybersecurity competencies, expand the depth of their Federal cybersecurity knowledge and experiences, and strengthen their skills. It will allow current Federal employees to gain exposure to a range of cybersecurity functional areas to improve their cybersecurity perspective and learning agility through stretch assignments. The program will also expand upon the successful Federal Cybersecurity Reskilling Academy, executed by OMB, OPM and the Department of Education in FY 2019, DHS will develop non-cyber federal employees who are interested in a cyber-career and have the necessary competencies by assessing their capability and aligning training and career broadening opportunities to develop them into cyber practitioners. Participants will gain development and skill enhancement through required and blended learning approaches such as work role-specific tours, conferences, cohort networking and training events, leveraging web-based virtual labs, and mentoring, in addition to the on-the-job experience. CISA is working alongside the Department of Veterans Affairs and Department of Defense to create career pathways using the NIST NICE Cybersecurity Workforce Framework, which build upon the workforce development programs suggested in the report's recommendations. CISA looks to continue to build upon training and education programs that transform, elevate, and sustain the learning environment to grow a dynamic and diverse cybersecurity workforce. Further, the CISA is working with the Department of Veterans Affairs, Department of Defense, and Office of Personnel Management to identify and leverage tools to assess aptitude and skills related to cyber positions. Many of these efforts, including the cataloguing of cybersecurity positions using the NIST framework, the rotational program and the reskilling academy are highlighted in the Administration's Solving the Federal Cyber Workforce Shortage paper included in the June 2018 Delivering Government Solutions in the 21st Century. In a field that experiences as much change as cybersecurity, updating employee skills that will be critical as the threat landscape evolves is important. However, employee development can have a beneficial effect on retention. Providing a well-defined career path, as well as associated trainings, that clearly map how a cybersecurity employee can grow within the organization, may contribute to retention. If provided a path to improve, acquire new skills, and progress along an exciting career path, whether it be technical or leadership in nature, employees will stay engaged and thus will be less likely to separate. Support to publish these career pathways on the NIST NICE website will benefit both the public and private sector. CISA believes it has exercised all available opportunities to recruit and retain talent to the extent allowable.Finally, investment in the re-

sources necessary for the HR IT to recruit and serve existing employees is critical to success. The current DHS HR IT solutions are predominately disjointed and some business processes are still paper-based; which adversely impacts the ability of DHS HR professionals to deliver high quality, effective services to the DHS workforce, including the recruitment and hiring of highly skilled personnel to meet the DHS mission. The Administration has recognized this and has included an increase of $10.5M in the DHS Management Directorate's Fiscal Year 2021 Budget to continue enhancements of the HR IT Portfolio and provide advanced automation capabilities across the DHS HR community, DHS workforce, and in some cases, family members of the DHS workforce. These improvements will provide DHS employees with self-service capabilities and will have profound effects on the DHS workforce and its readiness to support the DHS mission. This funding will support recruitment requirements and allow for a top-notch customer service organization capable of supporting a workforce to be on par and consistent with its private sector competition. CISA will work through the budget process to support this critical investment moving forward.

Ms. HOULAHAN. Google has announced that they are considering making change to the DNS settings on their Chrome browser and Android operating system that would, reportedly, have the effect of displacing DNS services provided by ISPs and other third parties and making Google the centralized encrypted DNS provider by default for most of the Internet. Is DHS/CISA aware of Google's plans? What are some of the implications of Google's plan to centralize DNS data? Specifically, how will Google's plan affect malware detection tools used to protect this nation's Critical Infrastructure?

Ms. MANFRA. The characterization that Google will become "the centralized encrypted DNS provider by default for most of the Internet" is incorrect. Google's plan, as shared in a September 10 blog post, is that the DNS settings for Chrome will be upgraded to a secure connection, only if the current DNS provider offers a secure connection. As Kenji Baheux, Chrome Product Manager, says in the post, "the DNS service will not change, only the protocol will. As a result, existing content controls of your current DNS provider, including any existing protections for children, will remain active." The post then describes in greater detail how this will occur and provides steps for users who prefer an insecure connection to opt-out. Microsoft has also made an announcement to offer DNS over HTTPS at the operating system level in a similar way Chrome does it within the browser. Mozilla Firefox is planning a change that would move users by default to a single, encrypted DNS provider, but Mozilla offered extensive documentation to continue supporting enterprise IT use cases; network-provided DNS can still be made mandatory. While only a single DNS provider is currently offered, Mozilla has made clear they are "working to build a larger ecosystem." CISA believes both approaches are thoughtful and helpful in driving users to more secure services. However, CISA also recognizes the side effects of increased DNS-over-HTTPS (DOH) use can cause—those enterprises that do not manage their assets effectively to lose visibility into DNS traffic leaving their endpoints. This also may inhibit CISA's ability to prevent malicious domains from resolving in civilian executive branch networks using EINSTEIN 3 Accelerated intrusion prevention capabilities. Centralizing DNS resolution to any service operator could provide that entity with unique insights into the DNS behavior of users. It could also deprive enterprise network security operations, cybersecurity service providers, and internet service providers of that same insight. However, as noted, enterprise policies can still be set on managed devices to require the use of an enterprise's preferred DNS provider. At the same time, CISA believes that Google and Mozilla's effort is intended to have positive security and privacy impacts of individual end users of their products, and to improve the performance of their systems. Not all malware detection mechanisms rely on the analysis of DNS activity. CISA has always recommended that critical infrastructure organizations thoughtfully employ defense-in-depth strategies that allow for the detection and prevention of unauthorized access by multiple means. However, in cases where DNS monitoring is used to detect unauthorized activity on Android devices and the Chrome web browser in the business networks of critical infrastructure entities, Google's plan could create a blind spot for network security analysts where those devices are not configured to abide by enterprise policies.

Ms. HOULAHAN. The process of DNS resolution today is very decentralized—it involves many DNS resolvers working in concert to power the Internet for this country and globally. What impact would centralization of DNS resolution would have in terms of our nation's cyber preparedness, resiliency, and security?

Ms. MANFRA. CISA seeks to champion technologies that help secure DNS and does not intend to re-engineer the distributed architecture of DNS infrastructure. Our intent is to re-route federal DNS traffic from untrusted service providers (some of which may be owned and operated by foreign entities), to trusted, U.S. owned recursive DNS service provider. CISA provided service will still offer distributed and resilient infrastructure in order to support our nation's preparedness, resiliency, and security. The service will provide managed federal DNS infrastructure that supports the latest DNS technologies (e.g. DNS over HTTPS and DNS over TLS), applies consistent protections and state of the art threat feeds, and provides CISA with visibility into the federal DNS traffic for analysis and feature enhancements.

Ms. HOULAHAN. I also serve on the Foreign Affairs Committee. I am curious what collaboration has looked like and will look like for each of your respective agencies as the Department of State stands up the Bureau of Cyberspace Security and Emerging Technologies and as other agencies consider creating similar teams? Further, do you see a need for the Presidential Policy Directive 21 (PPD–21), which divvies up responsibilities within the Federal Government for cyber, to be updated to reflect the emergence of these new departments?

Ms. RINALDO. NTIA does not see a need to revise PPD–21 based on the creation of new agencies. PPD–21 is flexible in that it assigns general responsibilities primarily at the department level, and relevant new agencies would be tasked at the direction of their departmental leadership. NTIA collaborates regularly with departments and agencies on cybersecurity issues. Newly established agencies' missions will be incorporated into the interagency policy process and work flow.

Ms. HOULAHAN. The process of DNS resolution today is very decentralized—it involves many DNS resolvers working in concert to power the Internet for this country and globally. What impact would centralization of DNS resolution would have in terms of our nation's cyber preparedness, resiliency, and security?

Ms. RINALDO. NTIA is actively monitoring recent protocol developments and implementations to encrypt Domain Name System (DNS) queries, such as DNS-over-Transport Layer Security and DNS-over-Hypertext Transfer Protocol Secure. NTIA staff regularly consult with DNS technologists and experts to understand the impact that new DNS security implementations may have on the Internet ecosystem. The Internet's decentralized architecture, including the DNS, Transmission Control Protocol/Internet Protocol, and physical infrastructure, has been one of its greatest strengths. It has contributed to innovations in connectivity and network performance, allowing companies to pursue economies of scale in telecommunications, content delivery, Web services, and other sectors and to offer greater connection speed and reliability for American consumers. The new protocol implementations represent a shift from current DNS resolution practice, but NTIA is closely monitoring these developments and working to ensure that such implementations do not introduce cyber threats to the Internet ecosystem or compromise its overall resiliency and security.

Ms. HOULAHAN. I also serve on the Foreign Affairs Committee. I am curious what collaboration has looked like and will look like for each of your respective agencies as the Department of State stands up the Bureau of Cyberspace Security and Emerging Technologies and as other agencies consider creating similar teams? Further, do you see a need for the Presidential Policy Directive 21 (PPD–21), which divvies up responsibilities within the Federal Government for cyber, to be updated to reflect the emergence of these new departments?

Mr. WILSON. DOD has been apprised of Department of State plans to reorganize internally. DOD does not anticipate a change in how DOD interacts with the Department of State on cyberspace issues as a result of the reorganization. At this time, because broad department responsibilities will not change as the result of internal departmental organizational changes, DOD does not anticipate a need to update PPD–21. Further, DOD encourages the critical infrastructure Sector Specific Agencies (SSAs) identified in PPD–21 to establish or bolster cybersecurity and cyber resilience measures to assure the protection and continued function of systems, capabilities, and assets for which they are responsible. Through a series of pathfinder initiatives, DOD is focused on improving its collaboration with DHS, other SSAs, and appropriate private sector entities—including select critical infrastructure partners—by sharing threat information, conducting collaborative analysis of vulnerabilities and threats, and, when authorized, mitigating those risks. These pathfinders, in turn, enable DOD and its Federal partners to leverage private-sector threat information to support DOD's mission.

Ms. HOULAHAN. In nuclear policy, the concept of deterrence is founded in our understanding of our adversaries' nuclear capabilities and our adversaries' understanding our own nuclear capabilities. It is my understanding that we don't have as thorough an understanding of our adversaries' capabilities when it comes to cyber. What work is being done to establish global nuclear norms? What steps are being taken to improve our partners' cybersecurity capabilities, especially those countries at most risk of cyber attack from our adversaries? Which department or agency is leading that effort?

Mr. WILSON. The Department of Defense works closely with the Department of State to deter malicious cyber activity and foster stability in cyberspace in part through the identification and promotion of peacetime norms of responsible state behavior in cyberspace. The 2015 report of the United Nations Group of Government Experts (UN GGE) on Information and Communications Technologies in the Context of International Security was instrumental in promoting certain cyberspace norms, and the GGE process is scheduled to resume in December 2019. As the lead foreign affairs agency, the Department of State has the lead role in coordinating foreign assistance, including cyberspace-related capacity-building assistance for international partners. DOD works to build the cyber capacity of its international partners, and the 2018 DOD Cyber Strategy lists expanding DOD cyber cooperation with international partners as one of the Department's key cyberspace objectives. DOD recently issued DOD International Cyberspace Security Cooperation Guidance to DOD components to facilitate and prioritize cyberspace capacity-building with allies and partners.

Ms. HOULAHAN. The process of DNS resolution today is very decentralized—it involves many DNS resolvers working in concert to power the Internet for this country and globally. What impact would centralization of DNS resolution would have in terms of our nation's cyber preparedness, resiliency, and security?

Mr. WILSON. Centralization of Domain Name System (DNS) resolution offers the idea of improved efficiency of system administration and has the potential to reduce the costs for resources. However, the impact of centralization of DNS resolution comes at the expense of security. Further, having a national or international centralized DNS name space would not be scalable. The DNS hierarchy was designed to be distributed; this distribution provides technical diversity, resiliency, and stability.

DNS centralization would result in greater vulnerability of specific targeted attacks and could increase the risk and threat levels. Globally, any attempt by one country to centralize DNS of independently managed country code domains and generic database Top Level Domains would most likely not be approved by the multistakeholder Internet Governance organizations and model that governs today's Internet. To clarify, a centralized DNS created by the United States would likely create opposition by foreign entities (e.g., countries, corporations). This would likely culminate in the generation of a fragmented or splintered Internet.

○