AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

[H.A.S.C. No. 115–121]

INTERAGENCY CYBER COOPERATION: ROLES, RESPONSIBILITIES AND AUTHORITIES OF THE DEPARTMENT OF DEFENSE AND THE DEPARTMENT OF HOMELAND SECURITY

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES

MEETING JOINTLY WITH

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY

[Serial No. 115–78]

HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

HEARING HELD
NOVEMBER 14, 2018

U.S. GOVERNMENT PUBLISHING OFFICE
33–477 WASHINGTON : 2019

COMMITTEE ON ARMED SERVICES
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

ELISE M. STEFANIK, New York, *Chairwoman*

BILL SHUSTER, Pennsylvania
RALPH LEE ABRAHAM, Louisiana
LIZ CHENEY, Wyoming, *Vice Chair*
JOE WILSON, South Carolina
FRANK A. LOBIONDO, New Jersey
DOUG LAMBORN, Colorado
AUSTIN SCOTT, Georgia
JODY B. HICE, Georgia
(Vacancy)
JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JIM COOPER, Tennessee
JACKIE SPEIER, California
MARC A. VEASEY, Texas
TULSI GABBARD, Hawaii
BETO O'ROURKE, Texas
STEPHANIE N. MURPHY, Florida

KATIE SUTTON, *Professional Staff Member*
LINDSAY KAVANAUGH, *Professional Staff Member*
NEVE SCHADLER, *Clerk*

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
JOHN KATKO, New York
WILL HURD, Texas
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
CLAY HIGGINS, Louisiana
THOMAS A. GARRETT, JR., Virginia
BRIAN K. FITZPATRICK, Pennsylvania
RON ESTES, Kansas
DON BACON, Nebraska
DEBBIE LESKO, Arizona
BENNIE G. THOMPSON, Mississippi
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California

BRENDAN P. SHIELDS, *Staff Director*
STEVEN S. GIAIER, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
HOPE GOINS, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

JOHN RATCLIFFE, Texas, *Chairman*

JOHN KATKO, New York
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
BRIAN K. FITZPATRICK, Pennsylvania
DON BACON, Nebraska
MICHAEL T. MCCAUL, Texas *(ex officio)*
CEDRIC L. RICHMOND, Louisiana
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
VAL BUTLER DEMINGS, Florida
BENNIE G. THOMPSON, Mississippi *(ex officio)*

KRISTEN M. DUNCAN, *Subcommittee Staff Director*
MOIRA BERGIN, *Minority Subcommittee Staff Director*

CONTENTS

Page

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

Langevin, Hon. James R., a Representative from Rhode Island, Ranking Member, Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services 3
Ratcliffe, Hon. John, a Representative from Texas, Chairman, Subcommittee on Cybersecurity and Infrastructure Protection, Committee on Homeland Security 5
Richmond, Hon. Cedric L., a Representative from Louisiana, Ranking Member, Subcommittee on Cybersecurity and Infrastructure Protection, Committee on Homeland Security 6
Stefanik, Hon. Elise M., a Representative from New York, Chairwoman, Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services 1

WITNESSES

Manfra, Jeanette, Assistant Secretary, Office of Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security 8
Rapuano, Hon. Kenneth, Assistant Secretary of Defense for Homeland Defense and Global Security, and Principal Cyber Advisor, U.S. Department of Defense 10
Shwedo, Lt Gen Bradford J., USAF, Director for Command, Control, Communications and Computers/Cyber, Chief Information Officer, Joint Chiefs of Staff 12

APPENDIX

PREPARED STATEMENTS:
Jackson Lee, Hon. Sheila, a Representative from Texas, Subcommittee on Cybersecurity and Infrastructure Protection, Committee on Homeland Security 38
Manfra, Jeanette 46
Rapuano, Hon. Kenneth 55
Stefanik, Hon. Elise M. 35

DOCUMENTS SUBMITTED FOR THE RECORD:
[There were no Documents submitted.]

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:
Ms. Jackson Lee 69
Mr. Langevin 69
Mr. Larsen 69

QUESTIONS SUBMITTED BY MEMBERS POST HEARING:
Mr. Brooks 77
Ms. Stefanik 73
Mr. Suozzi 78

INTERAGENCY CYBER COOPERATION: ROLES, RESPONSIBILITIES AND AUTHORITIES OF THE DEPARTMENT OF DEFENSE AND THE DEPARTMENT OF HOMELAND SECURITY

HOUSE OF REPRESENTATIVES, COMMITTEE ON ARMED SERVICES, SUBCOMMITTEE ON STRATEGIC FORCES, MEETING JOINTLY WITH THE COMMITTEE ON HOMELAND SECURITY, SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION, *Washington, DC, Wednesday, November 14, 2018.*

The subcommittees met, pursuant to call, at 3:04 p.m., in room 2118, Rayburn House Office Building, Hon. Elise M. Stefanik (chairwoman of the Subcommittee on Emerging Threats and Capabilities) presiding.

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

Ms. STEFANIK. The subcommittee will come to order.

Welcome to this joint hearing of the Armed Services Subcommittee on Emerging Threats and Capabilities [ETC] with the Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection [CIP].

Today, we will examine interagency cyber cooperation and the roles, responsibilities, and authorities of the Department of Homeland Security [DHS] and the Department of Defense [DOD]. Holding this joint hearing has been a priority for this subcommittee for the past few months, and we are pleased that it has come together today.

This is a timely opportunity to hear about recent interagency coordination efforts, and the status of related FY [fiscal year] 2019 NDAA [National Defense Authorization Act] provisions. This is a critically important topic that will shape our oversight going forward as we consider the long-term policy frameworks needed for the United States cyber enterprise.

Our committee, and ETC in particular, has performed significant oversight of the cyber organization, operations, and mission force development within DOD. With this joint hearing, we can now take a broader focus on the cyber organization and capabilities within the entire United States Government.

Cyber threats posed by both state and nonstate adversaries continue to grow and evolve at a rapid pace. These threats are not just to our military weapons and systems, but also to our Nation's critical infrastructures. Attacks against the electric grid, the financial

sector, or our healthcare system, could have profound impacts on our daily way of life and economic security.

As we have seen in recent years, cyberattacks, such as WannaCry ransomware, can have significant adverse economic impacts, and bring the private sector and government services to a standstill. And since the average response time to detect a cyberattack is measured in months, not minutes or hours, we must improve our abilities to detect and respond to malicious cyber activity.

This year, three important cyber strategies were released by the White House, the Department of Defense, and the Department of Homeland Security. These strategies all recognize the importance of a whole-of-government approach to addressing the challenges posed by securing our Nation in cyberspace. They will be an important step in building a cohesive U.S. cyber enterprise.

And while this hearing today isn't solely about election security, it affords us the timely opportunity to hear about the significant interagency efforts recently aimed at ensuring the security of our 2018 midterm elections. Protecting the elections required a broad approach led by the Department of Homeland Security that included contributions from the Department of Defense and many other partners.

Our subcommittee, in collaboration with the Homeland Security Committee, have been active in addressing the issue of improving cooperation between the two departments. In this year's fiscal year 2019 National Defense Authorization Act, we established a pilot program that allows the DOD to provide technical cybersecurity personnel to the Department of Homeland Security in order to enhance security and resiliency of critical infrastructure. I look forward to hearing the status of this pilot program at this hearing.

Also in this year's NDAA, we created a National Security Artificial Intelligence [AI] Commission that will be important in identifying the impact AI will have in the cyber domain. As our adversaries continue to improve at increasing speeds, we must similarly grow our abilities to defend against these threats.

I believe that we will only be successful if the U.S. can leverage the capabilities and authorities of all its departments and agencies in a united approach. We must reduce wasted resources on overlapping and duplicative efforts in government to make sure that we are using our cyber defense resources sensibly.

Both agencies here today have made great strides in building their cyber capabilities over the last few years. To build upon that progress, I firmly believe we need to continue to work to build interagency partnerships to ensure that whole-of-government approach to countering this growing cyber threat.

Let me welcome our witnesses here today: Ms. Jeanette Manfra, Assistant Secretary for the Office of Cybersecurity and Communications at the Department of Homeland Security; Mr. Ken Rapuano, Assistant Secretary of Defense for Homeland Defense and Global Security, and Principal Cyber Advisor at the DOD; and Lieutenant General Bradford Shwedo, Director of Command, Control, Communications and Computers, Cyber, and Chief Information Officer [CIO] at the Joint Chiefs of Staff. We look forward to your testimony.

And before I turn to my friend and ranking member, Jim Langevin of Rhode Island, for his opening remarks, I want to take a moment to thank him for his hard work and dedication over the past 2 years of the 115th Congress. It really has been a highlight of my time in Congress working with you, Jim, and I look forward to partnering with you in the future in a collaborative and bipartisan approach.

I now want to recognize my friend, Jim Langevin.

[The prepared statement of Ms. Stefanik can be found in the Appendix on page 35.]

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

Mr. LANGEVIN. Thank you, Chairwoman Stefanik. And I want to begin by thanking you and Chairman Ratcliffe for convening the joint hearing on such an important topic. And likewise, I want to say what a pleasure it has been working with you over this—for the last 2 years as you chaired the subcommittee, and it has been collaborative and bipartisan, and I, too, look forward to continuing our working relationship as well. So thank you for that also.

So the challenges in cyberspace affect all aspects of our national and homeland security, and I am glad that these two subcommittees, both of which—on which I sit, are collaborating to better understand the cooperation between the agencies that we oversee.

I want to thank our witnesses for being here today as well, and I look forward to hearing your testimony.

But before I do go any further, I also must congratulate Chairman McCaul and Ranking Member Thompson of the Homeland Security Committee for their work shepherding the NPPD [National Protection and Programs Directorate] reorganization bill through the House last night. It has been a bit of a slog, as it often is with our friends on the other side of the Capitol, but after 3 years, I am proud they will soon be officially opening the Cybersecurity and Infrastructure Security Agency [CISA] at Department of Homeland Security.

The legislation headed by—the legislation headed to President Trump for his signature reaffirms Congress' intent that the Department of Homeland Security take the lead role in protecting civilian government and critical infrastructure, something I look forward to hearing more about from our witnesses today.

In particular, I would like to congratulate you, Assistant Secretary Manfra, and I hope that you will pass along my congratulations to Under Secretary Krebs as well. The new agency will be well served, I know, by your leadership as well as the inaugural executive team. So—and also, let me say what a pleasure it was to have you up in Rhode Island recently, and I appreciate your contributions there that you made to our Cyber Advisory Committee that I put together.

But beyond the implications of this is this existing new development. We are here this afternoon to discuss collaboration between two agencies with important but distinct cybersecurity roles. Now, again, I was privileged enough to have—to host Assistant Secretary

Manfra back in my district late last month to hear about some of this collaboration with respect to election security.

Our elections are obviously the cornerstone of our democracy and it is essential that they be protected from any interference, foreign or domestic. As we saw in 2016, the threat is real and it demands a whole-of-government response. Recognizing this, DHS and DOD worked together in the weeks leading up to the election to remove any legal or operational obstacles that would prevent timely defense support of civil authorities in the case of a cyber incident targeting our elections that exceeded DHS's asset response capabilities.

I was also pleased that DOD was able to work with National Guard personnel activated under State Active Duty status, including some of our excellent network defenders right in Rhode Island in order to share sensitive intelligence on Election Day.

The efforts of both those departments paid off. And due to their work and the diligence of local election officials, last week's voting went off without any major cybersecurity incident, but we cannot let the success blind us to the tremendous challenges that remain ahead.

As highlighted in the recent cyber strategies that have come out of DHS, DOD, and the White House, our adversaries continue to look for ways to gain an advantage by exploiting our vulnerabilities in cyberspace. And while Congress has been abundantly clear about DHS's primacy in defending civilian networks in the United States, coordination, collaboration, and information sharing with the DOD will be critical to the defense of the homeland.

So I hope to hear from our witnesses today how these collaborations are succeeding, and, frankly, where more work needs to be done. I want to better understand how, in a time of crisis, DOD will be able to prioritize the requests coming from DHS while achieving its mission to protect the DODIN [Department of Defense Information Network], the DIB [Defense Industrial Base], and other defense critical infrastructure, and maintain capability and capacity for conducting title 10 cyber operations.

So understanding that DHS can and must have the capability to take on more of the domestic mission without relying exclusively on DOD for support, I hope that witnesses will address that—what capability building is and should be going on to better empower the new CISA. I also hope the witnesses will talk about how they are ensuring collaboration works its way down to the operational level, so that Homeland Security equities are fully considered throughout the entire decision-making chain.

Recent policy developments from the administration, from national security policy memorandum 13, to the recently signed joint memorandum, will help frame the U.S. Government's collective response to cyber threats, and I trust the administration will be fully transparent with our committees in providing these documents and candid assessments of their implementation.

Finally, I look forward to hearing a status update on the report required in section 1653 of the FY 2019 NDAA about cyber civil support teams and the feasibility of using their unique authorities to better defend the Nation. So cybersecurity is a team sport; only by working together can we reduce our risk and ensure a bright fu-

ture where the internet remains open, reliable, interoperable, and secure.

So with that, again, I want to thank our witnesses for being here today, and I yield back to the Chair. Thank you.

Ms. STEFANIK. Thank you, Jim.

I want to welcome Chairman John Ratcliffe of Texas from the Cybersecurity and Infrastructure Protection Subcommittee of the Homeland Security Committee to today's hearing, and now I yield to him for his opening remarks.

STATEMENT OF HON. JOHN RATCLIFFE, A REPRESENTATIVE FROM TEXAS, CHAIRMAN, SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION, COMMITTEE ON HOMELAND SECURITY

Mr. RATCLIFFE. Thank you, Chairwoman Stefanik. I am excited to have the opportunity to hold this hearing with you. These joint events always provide some unique insights and perspectives that would be hard to explore under a single committee purview.

We are here today to discuss something that is vital to our national security. Cybersecurity affects every single American, every single day. That is because cybersecurity is national security. So it is imperative that the Department of Homeland Security and the Department of Defense work hand in glove to protect our Nation's systems and to provide assistance to our critical infrastructure partners.

That assistance comes in many forms, and that is part of the reason why we are here today: to explore the roles and responsibilities of the two departments, and to better understand how they can effectively and efficiently work together to keep our Nation safe from malicious cyber actors.

Whether we are talking about the Chinese stealing sensitive information on our Navy submarines or the Iranians attempting to target defense contracting systems, nation-state actors remain poised to use any cyber vulnerabilities or gaps in our defense to get a competitive advantage to use against us later.

That is why I am grateful to have representatives from the Department of Defense here today. I look forward to hearing how they, as the sector-specific agency, are partnering with the Defense Industrial Base to ensure that our Nation's capacity to wage war remains unmatched.

I am also pleased to have a representative from the Department of Homeland Security here to lay out the multitude of roles that DHS has in this space, and I am confident that Assistant Secretary Manfra will do her usual superb job of illustrating the Department's broad array of responsibilities and authorities. Those include overseeing all 16 critical infrastructure sectors, and partnering with industry to share information and build capacity, and protecting Federal networks from the daily inundation of cyberattacks.

The Department has statutory authority to carry out all of these responsibilities, and it is imperative that DHS continues to take the lead in this regard. A civilian-led system embodies the foundation that this democracy was built on.

Despite the respective individual roles, the most effective way to keep our country's cyber ecosystem safe is through DOD and DHS

cooperation. We can't have a stovepiping of efforts; we can't have a fractured set of agendas; and we cannot have a disjointed front line in defending against our cyber adversaries and threats.

We need to ensure cooperative approaches to cybersecurity, approaches like section 1650 of the NDAA which allows for DOD personnel to assist Homeland Security with cybersecurity-related efforts. This was an effective tool that was used to help bolster DHS's preparedness in the lead-up to the elections just last week.

There are other approaches, like project pathfinder, which seeks to keep our financial sector safe by streamlining information sharing, and using it to defend forward. I have faith that both departments can and will work through any growing pains that may be encountered. And I look forward to hearing from our witnesses today on both the past successes that we have had at keeping this Nation safe, but more importantly, on how we can continue that success going into the future.

Finally, in what is my last hearing as the chairman of this subcommittee, I want to thank all of the CIP members, both Republican and Democratic, for their excellent work this Congress. The 115th Congress has been defined by bipartisan success when it comes to legislation and oversight on the issue of cybersecurity, and our committee has paved that path.

I hope that we can continue to carry this momentum and energy forward into the 116th Congress, and work in a bipartisan manner to ensure the integrity of our national security because cybersecurity is national security.

Again, I thank our witnesses and I yield back.

Ms. STEFANIK. Thank you.

The gentleman from Louisiana, the Ranking Member, Cedric Richmond—actually, he is here. I was just going to put your opening statement in for the record. When you get up here, I will recognize you for any opening remarks.

STATEMENT OF HON. CEDRIC L. RICHMOND, A REPRESENTATIVE FROM LOUISIANA, RANKING MEMBER, SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION, COMMITTEE ON HOMELAND SECURITY

Mr. RICHMOND. Good afternoon. I want to thank Chairwoman Stefanik and Chairman Ratcliffe for holding today's joint hearing to assess interagency coordination of cybersecurity activities at the Department of Homeland Security and at the Department of Defense.

Last night, after years of debate and negotiation, Congress sent H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act, to the President's desk. This bipartisan legislation confirms, once again, that Congress intends for DHS to be the primary Federal civilian interface with the private sector on cybersecurity.

I look forward to working with DHS to help the Cybersecurity and Infrastructure Security Agency mature into an operational component and develop the capabilities needed to meet the challenges ahead, from securing election infrastructure to protecting the grid. The Department of Defense will be an integral partner as DHS carries out its mission to help secure civilian networks.

I understand that DOD and DHS recently signed an agreement clarifying how they will coordinate certain cyber activities. Although I have not seen that agreement, I am hopeful that it will provide clarity for the Department's roles and responsibilities. I look forward to reviewing the agreement and ask that it be submitted to our committee as soon as possible.

Moving forward, the success of DOD and DHS's collaboration rests on whether the following three things happen: One, DOD and DHS must implement the agreement of understanding at both the policy and operational levels; two, DOD and DHS must communicate and adhere to their respective roles and responsibilities as they engage with agencies across the Federal Government and with the private sector; and three, the administration must request and Congress must provide the funding and the resources necessary for DOD and DHS to carry out their missions.

To my first point, too often I hear testimony from principals about how well their agencies are coordinating, only to learn from folks in the field that it isn't the case. To me, the problem seems to be that as Federal agencies work to delineate roles and responsibilities on cybersecurity they reach an agreement on a policy level without involving the operational folks. That invites frustration, confusion, and, at times, mission creep.

Accordingly, I will be interested in learning how DOD and DHS plan to socialize their new agreement on cyber roles and responsibilities throughout their organizations, from policy operations and solicit buy-in.

On the second point, it is important that the respective cyber missions of DOD and DHS are communicated and clearly understood throughout the Federal Government and among critical infrastructure owners and operators. Toward that end, I will, once again, note my strong concern that the White House has eliminated the Cybersecurity Coordinator.

A White House Cybersecurity Coordinator would be in the best position to ensure the full capabilities from across the Federal Government are brought to bear to protect against cyber threats without sowing confusion about who should be doing what.

Finally, we have to provide DOD and DHS with the resources it takes to do their jobs. As everyone here will acknowledge, the cyber threats we are facing are evolving, and we have called on DHS to help secure the Federal Government, State and local governments, and critical infrastructure from breaches by state and nonstate actors. But DOD's cyber funding outpaces DHS's cyber funding by about 8 to 1. If we expect DHS to be DOD's civilian equivalent for cybersecurity, we need to fund it that way.

I thank the witnesses for being here, and I look forward to hearing their testimony.

With that, Madam Chairman, I yield back the balance of my time.

Ms. STEFANIK. Thank you, Ranking Member Richmond. Your time was perfect for your opening statement.

Immediately following the conclusion of this open hearing, the Members will transition to Rayburn 2212 for a closed, classified briefing from our witnesses.

Without objection, the witnesses' prepared statements will be made a part of the record. I ask that the witnesses please try to keep your remarks to no more than 5 minutes.

And, Ms. Manfra, we will begin with you. You are recognized for 5 minutes.

STATEMENT OF JEANETTE MANFRA, ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. MANFRA. Thank you, ma'am.

Chairman Ratcliffe, Chairwoman Stefanik, Ranking Member Richmond, Ranking Member Langevin, and members of the committee, thank you for today's opportunity to testify regarding the Department of Homeland Security's ongoing and collaborative efforts to strengthen the cybersecurity of our Nation's critical infrastructure. This is a core Homeland Security mission.

But first, I would like to thank you for your leadership on establishing the Cybersecurity and Infrastructure Security Agency at the Department. The National Protection and Programs Directorate will now have a name which accurately reflects the reality of what we do: We secure cyberspace, the institution, systems, and services that help businesses thrive, and government, of all levels, operate.

Last night the House passed the legislation by unanimous consent, and the bill is now headed to the President's desk. This accomplishment could not have been achieved without the strong leadership of our partners here in the House of Representatives, and we know this demonstrates your own commitment to ensuring our national security.

For the last 10 years, I have worked to advance the Department's cybersecurity and critical infrastructure mission. Prior to joining DHS, I was an Army officer, so I believe I have a unique perspective on how we can better strengthen the DOD and DHS partnership, and I am personally invested in making this happen.

I am proud of the progress that we have made to date, and looking forward to talking more about our progress ahead. Cybersecurity threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety.

Rarely is a cyber event sector-specific. Our adversaries target systems that are cross-sector, and the growing interdependencies of cross-sectors demand an integrated approach. Establishing CISA highlights the central role we play across the Federal Government and our responsibility to all critical infrastructure in making manifest this integrated approach.

As we have learned, the information in Federal operations must not be siloed. This is one of the key lessons learned from 9/11. To combat a threat that is transnational and operates in the seams between agencies and the public and private divide, a whole-of-nation approach is required. We see these same lessons applied, amplified by the speed of technological change to cyberspace.

At NPPD, and soon at CISA, our vision is to fully realize this national effort, challenging old organizational institutional divides

across the Federal Government and between the public and private sectors that impede our ability to provide for a collective defense in cyberspace.

Collective defense, the idea that the risks we face in a dense, interconnected, technological environment are shared, is the only model and way forward. Threats and risks do not conform to our divisions; neither should we. We believe it is our responsibility to make this a reality. We will forge a national understanding of threat and risk and coordinate across the Federal Government and private sector to detect and respond to cyber threats wherever they occur.

We serve as an information and operations integrator focused on delivering organization-specific and cross-sector risk management support to enhance the resiliency of our Nation's critical infrastructure. Our National Cybersecurity and Communications Integration Center, or the NCCIC, provides a broad range of capabilities to assist private sector entities across all sectors of critical infrastructure, including energy, finance, communications, emergency services, and health care.

It is best to think of the NCCIC as the point of fusion for cybersecurity threat detection, response, and coordination for both the public and the private sectors. We bring together the intelligence community, law enforcement, sector-specific agencies, international partners, the private sector, and the Department of Defense to carry out this mission.

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.

DHS and DOD recently finalized agreement, which reflects the commitment of both departments in collaborating to improve the protection and defense of the homeland from strategic cyber threats. This agreement clarifies roles and responsibilities between our organizations to enhance our government's readiness to respond to cyber threats and establish coordinated lines of efforts to secure, protect, and defend the homeland.

In order to achieve these objectives, our departments are adopting a threat-informed, risk-based approach that ensures the resilient delivery of national critical functions and services. We 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.

Based on this prioritization, we will forge a common understanding of strategic cyber threats that can enable private sector network defenders, critical infrastructure owners and operators, and government actors to proactively secure their networks and operations.

And finally, our departments are coordinating to inform and mutually support our respective planning and operational activities. With our knowledge of the domestic risk landscape and our work with the private sector we will inform DOD's "defend forward" ef-

forts to preempt, defeat, and deter malicious cyber activity outside the U.S. that is targeting our critical infrastructure.

And DOD's "defend forward" operation will inform and guide our efforts at DHS to anticipate adversary action, understand potential risk to critical infrastructure, and empower our private sector stakeholders with the information they need to secure their enterprise.

Our vision is to continue to be the central axle for cybersecurity across the Federal Government, ensuring both Federal and private sector partners have a full and complete understanding of the threats we face and are prepared to defend against them.

I look forward to further outlining our efforts to safeguard and secure cyberspace. Thank you. I look forward to your questions.

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

Ms. STEFANIK. Thank you.

Mr. Rapuano.

STATEMENT OF HON. KENNETH RAPUANO, ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY, AND PRINCIPAL CYBER ADVISOR, U.S. DEPARTMENT OF DEFENSE

Secretary RAPUANO. Chairwoman Stefanik, Chairman Ratcliffe, Ranking Members Langevin and Richmond, and members of the committees, thank you for your opportunity to testify on interagency cyber cooperation between the Department of Defense and the Department of Homeland Security.

Last week's midterm elections serve as a timely inflection point to review the close collaboration between our two departments. I appreciate the opportunity to discuss the sea change in our partnership, and thank you for your broad and continued support for the Department's cyber missions.

Before reviewing the Department's strategic posture for cyberspace, I would like to offer a few observations on the threat environment. As the National Defense Strategy and the 2018 DOD Cyber Strategy make clear, the 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 infrastructure, and reduce our economic prosperity. In particular, we are engaged in a long-term competition with China and Russia. These states have expanded the competition to include persistent campaigns in and through cyberspace with activities that individually fall below the threshold of armed conflict but collectively pose a long-term strategic risk to the Nation as well as to our allies and partners.

Nested within the National Security and National Defense Strategies, the 2018 DOD Cyber Strategy prioritizes the challenge of great power competition, and recognizes that the Department must adapt a proactive posture to compete with and counter determined and rapidly maturing adversaries.

It makes clear that DOD's focus on cyberspace, like in other domains, is to defend forward. That is, to prevent or mitigate threats before they reach American soil. This focus complements the DHS

cybersecurity strategy's emphasis on domestic preparedness and risk management.

Together, the DOD and DHS strategies form a natural, mutually supporting approach to defense in depth. With these new strategies in place, DOD and DHS have worked together to establish a framework to drive domestic preparedness and critical infrastructure protection efforts.

Secretary Mattis and Secretary Nielsen recently signed a joint memorandum that frames how DHS and DOD will secure and defend the homeland from cyber threats. This is a major step forward in fostering closer cooperation, and marks a sea change in the level of collaboration between our departments.

Implementation of the joint memo is already underway. Yesterday, I joined my DHS and Joint Staff colleagues to sign the joint DOD–DHS Cyber Protection and Defense Steering Group Charter. Established at the direction of Secretaries Mattis and Nielsen, this steering group will apply senior leadership energy to enhance the U.S. Government's readiness against cyber threats.

This fall, Department of Defense and DHS cooperated closely to ensure that all appropriate Federal Government tools and resources were available to protect and defend the 2018 midterm elections from foreign interference. DOD provided standing approval for DOD personnel to support DHS cyber incident response activities in the event a significant cyber incident impacted elections infrastructure.

The National Guard also played an important role in election support. Governors from several States used National Guard personnel in State status to support election cybersecurity in accordance with State law and policy.

Beyond elections, DOD is focused on how to improve collaboration with DHS and the critical infrastructure sectors. Through a series of pathfinder initiatives, we are enabling private sector entities to defend their networks by sharing relevant threat information. In turn, these pathfinders will enable the Department of Defense to leverage private sector threat information to inform DOD cyberspace operations.

We are also strengthening the Defense Industrial Base sector partnership to improve the security and resilience of the Defense Industrial Base critical infrastructure. This approach aligns with the National Defense Strategy guidance to enhance joint force lethality and reform departmental procedures.

DOD is coordinating with DHS's National Policy and Programs Division to establish a joint plan for future cyber incident response. By identifying roles, responsibilities, and coordination mechanisms, we are establishing a baseline for efficient and effective interagency operations.

Lastly, I would be remiss if I didn't highlight the National Guard's contribution to DOD and the Nation. We fully recognize the National Guard's two complementary roles as an integral part of the total force and as a State capability.

Section 1653 of the FY 2019 NDAA, which requires an assessment of the feasibility and advisability of establishing cyber civil support teams, provides an opportunity to review and refine the role of the National Guard. My team will lead this review.

Thank you again for the opportunity to appear before you today. As you can see, the Department has undertaken extensive work with DHS to improve defense of the homeland and national critical infrastructure, but there is much left to do. I look forward to working with Congress as we address the challenges facing the homeland, and I welcome your questions today. Thank you.

[The prepared statement of Secretary Rapuano can be found in the Appendix on page 55.]

Ms. STEFANIK. Thank you.

Lieutenant General Shwedo.

STATEMENT OF LT GEN BRADFORD J. SHWEDO, USAF, DIRECTOR FOR COMMAND, CONTROL, COMMUNICATIONS AND COMPUTERS/CYBER, CHIEF INFORMATION OFFICER, JOINT CHIEFS OF STAFF

General SHWEDO. Chairwoman Stefanik, Chairman Ratcliffe, Ranking Members Langevin and Richmond, and members of the committees, good afternoon and thank you for the opportunity to testify today on the Department of Defense and Department of Homeland Security cyber collaboration and information sharing.

I would like to take this opportunity to thank Congress for its quick action in improving the National Defense Authorization Act for fiscal year 2019, providing new authorities that allow the joint force to conduct cyberspace operations to disrupt, defeat, and deter malicious cyber activities. Thank you for your broad and continued support.

Since the elevation of United States Cyber Command [CYBERCOM] from a sub-unified command to a combatant command, cooperation on cyber issues between DOD and DHS have been streamlined through Cyber Command, and it has prospered. Close cooperation between the departments has exponentially added value in areas such as intelligence sharing, cyberspace operations, and cyber policy development.

As Mr. Rapuano indicated, midterm elections provided a real-world platform to showcase interdepartmental collaboration in cyberspace. The cyberspace capabilities of the Department of Defense and DHS has increased through partnership and working together to secure the Nation's election systems.

The 2018 National Defense Strategy, 2018 DOD Cyber Strategy, and the draft 2018 National Military Strategy all reflect what DOD senior leaders refer to as a changing nature and character of war. Russian and Chinese military thinkers have closely studied the United States and devised strategies to achieve their objectives short of armed conflict. They are doing this with actions below the threshold of armed conflict, leveraging propaganda, diplomacy, economic pressures, and threats to coerce nations.

Our joint forces need the best intelligence, information technology [IT], and training, and they need it quickly. The joint force is committed to act in concert with our interagency partners to share threat intelligence to enhance the whole-of-government defenses and our collective ability to respond to malicious cyberspace activities.

Sharing intelligence, indications, and warning are one of six lines of effort specified in the joint memorandum between DOD and DHS

referenced by ASD [Assistant Secretary of Defense] Rapuano earlier. Together, the joint memorandum and charter provide guidelines to vector the departments in sharing information, reducing the timeline on actionable intelligence, and paving the way for proactive collaboration in the defense of our Nation.

This requirement to share intelligence and information is bidirectional, and it is not confined to the sectors owned and operated by DOD and DHS. To that end, we are engaged to set pathfinder efforts with DHS and with sector-specific agencies charged with the security of critical infrastructure.

The National Defense Strategy establishes the Chairman of the Joint Chiefs of Staff, General Dunford, as the global integrator with the understanding that the evolved nature and character of war make it unlikely that the impacts of a conflict will be confined to a single geographic area of operation.

The U.S. homeland can now be impacted directly by events that 20 years ago would only generate indirect or collateral effects. In the cyber domain, this shift requires the joint force to take on at least two additional roles: one is the global integration in cyber and the other is coordination of cyberspace activities.

The Joint Staff is taking on the global integration role to synchronize collaborative efforts to ensure impacts from one theater of operations does not affect the other, and are intentional and supportive rather than collateral.

During the closed-door session, I will provide operational details regarding ongoing efforts that illustrate the close cooperation among the departments with regard to election security and critical infrastructure pathfinders.

Thank you again for the opportunity to appear before you today. Our relationships with Federal, State, local industry and international partners is critical to everything the Department is doing in the cyber domain. We appreciate your continued strong support in providing the authorities that allow us to strengthen these partnerships and build strong programs to protect and defend our Nation.

I look forward to your questions. Thank you.

Ms. STEFANIK. Thank you to each of the witnesses for your testimony.

My first question has to do with many of the themes we have heard already, is this whole-of-government approach. Obviously, we need to ensure that we are not siloing information, but at the same time, we also need to ensure that we are not seeing mission creep, because when it comes to our oversight and our jurisdiction, we want to make sure that each agency has the resources available for each department.

But I would like to know what efforts are being taken to ensure that each department focuses specifically their efforts on their lanes of responsibility to prevent mission creep. Ms. Manfra, we will start with you.

Ms. MANFRA. Thank you, ma'am, for the question.

I think what we have decided to do is take real-world scenarios. And so we talked a little bit about the pathfinder initiatives, also with the elections, but working through specific real-world areas where we do need to share information, and having both the law-

yers and the operators working side by side, working with the operators in terms of what information would be useful for you to have access in order to do your job, and then working with the lawyers to ensure that we are not going outside the bounds of what is appropriate from an authority perspective.

And I defer to my DOD colleagues. We feel very comfortable that this is the right approach. And as we learn from each one of these sort of initiatives, whether it is with the financial sector or the energy sector or elections, we are learning lessons that can be applied more broadly.

Ms. STEFANIK. Mr. Rapuano.

Secretary RAPUANO. So we are extremely conscious of what our focus and priority is in terms of defending the Nation against exigent threats. The transformation in terms of the way the Department of Defense looks at the homeland with regard to vulnerability to cyber, particularly with regard to critical infrastructure, is that significant threat to national critical infrastructure is a national security concern.

It remains a DHS mission, and the role that we play and that we very clearly defined in all of our engagements as well as the memorandum of understanding with DHS is that we provide civil support to civil authorities in those cases, in those areas where the needs exceed DHS capability and their unique skills and capabilities that the Department offers.

Ms. STEFANIK. Lieutenant General Shwedo, did you want to add?

General SHWEDO. Sure. You know, just one point that Ranking Member Richmond brought up. Often, there is a frustration because we go through exercises to try and figure out some of the details of these relationships. These elections gave us a real-world platform where we started working out a lot of these things.

And we actually had a meeting yesterday where we sat down, and there isn't always concurrence on a point of view. The good news is, we are taking these opportunities in a real-world scenario as opposed to some theoretical wargame, and I feel we are gaining a lot of ground.

And actually, there was a discussion about letting our staffs come together and make out the equivalent of a three-ring binder and figure out so we can move very fast with, "We think it is scenario B," bang, so we can get them faster, in their lane, the support they need, and the mission set associated with it. So once again, we are taking advantage of the opportunity right now.

Ms. STEFANIK. And my last question in the minute I have left, we have heard in previous hearings and briefings that there is no common cyber operating picture that is shared between DOD, DHS, and FBI [Federal Bureau of Investigation]. What efforts are being taken to address this shortfall?

Ms. MANFRA. I can start, ma'am. You know, I think whether we—there are tools that are available to have a common operational picture in terms of incidents that we are working to share, but it does get back to the earlier point, is we have to be very precise in terms of what information agencies have the authority to view.

And so we are working very closely—kind of going back to that—what do the operators need to do their mission and then, how do

we create the environment where we can share the information appropriately, so ensuring names are anonymized and those types of things. And so I think we have made more progress in this area than we have in the previous decade in just the last few months, very much focused on the elections.

But that is how we are approaching it in terms of we have great technology that is available to us and that allows us to share information, that allows us to look for patterns, those types of things. We want to leverage that, but we have to do it in the appropriate legal frameworks. And so we are getting all those lawyers and operators together to work through specific instances to make sure we can get to that common view.

Ms. STEFANIK. Thank you. My time is about to expire.

Mr. Langevin, you are recognized.

Mr. LANGEVIN. Thank you, Madam Chair.

Ms. Manfra, one of the key challenges we face with interagency cooperation is prioritization given limited resources and agencies with different mission sets. So how is the standup of the new National Risk Management Center helping to inform efforts to understand the vulnerabilities of critical functions, and how are you ensuring that these lessons are diffused throughout the interagency, particularly through the Department of Defense?

Ms. MANFRA. So the work of the National Risk Management Center is filling a key gap that we identified, which was looking at the systems and the functions across the country. So it is taking a more functional approach instead of thinking about specific assets or organizations, but it is looking at defining what we are calling national critical functions as one of its key efforts.

And that effort working with industry will then be able to inform how our department, how other departments and other sector-specific agencies, such as DOD, are participating in this. And so we are defining it from a mission and industry from a business perspective, and then once we have these national critical functions identified, which we will have by the end of the year, then we are going to assess the risk to those. And DHS and DOD will be working this together, and as well as other agencies that have a role in there.

And then that starts to be able to trickle down, and so that we can focus on are we prioritizing all of our resources towards protecting and preparing ourselves for responding to the, you know, disruption or the denial of some of those key functions and services. So that is really the—kind of the core of the National Risk Management Center, and it is how it is going to help inform myself, but also the other agencies.

Mr. LANGEVIN. Okay. And to both you and to Mr. Rapuano, I am pleased obviously that Secretaries Mattis and Nielsen have recently signed a joint memorandum. We have discussed that, touched on that a bit today, and I certainly look forward to reviewing it. How are your departments working to ensure that collaboration goes beyond just the principal level and happens operationally as well?

Ms. MANFRA. From my perspective at DHS, the core of the collaboration is actually happening at the operational level. Our Deputy Director for Operations within the NCCIC has been our lead

for collaborating with her counterparts across DOD. And then we are identifying other collaboration points, so whether that is on the operation side or the planning elements, and then the steering group will be that mechanism by which we oversee that collaboration and ensure that we are actually making tangible progress on these outcomes. But much—the bulk of what we are doing is actually happening at the operational level.

Mr. LANGEVIN. Okay.

Secretary RAPUANO. I would echo that. Our staffs work very closely in terms of in my organization, as well as the Joint Staff. The real working level work is at U.S. Cyber Command working with Secretary Manfra's folks on the operational piece of the equation.

We also have direct interests at the Department of Defense as the sector lead for the Defense Industrial Base, and we are collaborating more and more on that, based on the threats that are manifesting associated with, again, particularly Russia and China, as well as defense-critical assets for which we have dependencies on commercial-critical infrastructure. So that is another area of focus and area of collaboration with DHS.

Mr. LANGEVIN. So I may come back to a couple questions, but I wanted to get this clarified, too. Mr. Rapuano, what is the status of the report required in the FY 2019 NDAA on cyber civil support teams?

Secretary RAPUANO. So we are currently working that—the response to that. I can get you the details in terms of when specifically we will be getting that to you.

[The information referred to can be found in the Appendix on page 69.]

Mr. LANGEVIN. Okay. That is something that we would need to follow up on, and I just want to get a status report, and we look forward to seeing the final version.

But let me go back. Mr. Rapuano, can you describe your approach to bringing DHS in on pathfinder conversations with the financial sector and DOE [Department of Energy]?

And, Ms. Manfra, if we have time, can you—can we better—how can we better ensure DHS's unique perspective as the Federal lead for cyber defense is represented in interagency policy decision making, especially when the Department's—our relative newness with—the Department's relative newness means that it has not traditionally been included? Mr. Rapuano.

Secretary RAPUANO. I would just start by saying, with regard to the pathfinder and financial sector, it wasn't a question of bringing DHS in. We were engaged from the very beginning with DHS on that, as well as the Department of the Treasury.

One of the interesting facets of the financial sector is they have a very sophisticated—significant investments in cyber protections. And the outlook and approach there was looking at what best practices may they have developed because of the time and attention they played that we could be applying to other critical infrastructure sectors.

And the energy focus for both of us is a high priority, because energy is considered to be really one of the fundamental foundational elements of critical infrastructure for which many of the oth-

ers depend on. So, again, that has been something we have been engaging with DHS on from the beginning.

Mr. LANGEVIN. Thank you.

Ms. MANFRA. I can answer very briefly. We are absolutely included in all the relevant conversations related to cyber operations, whether those are at the NSC [National Security Council] or with DOD or other agencies. While we are new, we—you know, we have a Secretary who is very knowledgeable in cyber and myself and my boss, Under Secretary Krebs. We are in every one of those conversations where we need to be.

Mr. LANGEVIN. Thank you.

Ms. STEFANIK. Mr. Ratcliffe.

Mr. RATCLIFFE. Thank you, Chairwoman.

Ms. Manfra, I want to start with you. It has been publicly reported that 50 DOD personnel were reassigned to the NCCIC in the lead-up to last week's midterm elections. Can you go into a little more detail into the nature of their mission within DHS during that time? I am curious what operational role DOD personnel played, if any, that wasn't just situational awareness.

Ms. MANFRA. We had 11 personnel that came over, integrated. We do have liaison officers that have been long established with DOD that come from CYBERCOM. They have been integrated.

Part of the conversation that we had in pre—in setting up prenegotiating, if you will, the requests for assistance, should we need it, if we needed search support on Election Day or after, was that it would be helpful to have some DOD personnel that would be fulfilling that request to have some familiarity with our organization. So they came over for a couple of days just to become a little bit more familiar. They are still serving in that liaison role, but it was about 11 people that did come over.

Mr. RATCLIFFE. Okay. I want to follow up a little bit on the discussion about pathfinder as it relates to the financial sector. As you know, Cybersecurity Act of 2015 offered liability protections to private organizations for sharing cyber threat information with DHS.

And that protection, of course, was intended to incentivize the private sector companies to share information with the Federal Government. But I am not sure—I am a little concerned that the financial sector organizations are sharing information directly with DOD, and I am wondering, if that is the case, are those organizations still offered liability protections?

Ms. MANFRA. To be clear, sir, they are sharing it with DHS. We are partnering with DOD in, as I mentioned, working through the legal constructs to ensure that DOD can have access to the information as well. So it is sort of the through the DHS framework and the construct that we are bringing DOD into being a part of.

I would defer to DOD on the liability protections.

Mr. RATCLIFFE. Do you want to expand on that?

Secretary RAPUANO. I am not tracking the liability protections, but as Secretary Manfra notes, we really work with and through DHS in terms of the interface with the private sector. We bring the expertise and unique capabilities that the Department has, but we are very conscious of not crossing over the lines in terms of sensitive or proprietary information. So we really use DHS as a gatekeeper or filter, so to speak.

Mr. RATCLIFFE. Okay. So let me follow up on that with you, Mr. Rapuano, and you, General Shwedo, in terms of, you know, what we are hearing from DHS stakeholders is that there is a general agreement about rules of the road at the high level, but maybe not at the command level. So I am thinking of responses to domestic cyber activity like the ransomware attack on the city of Atlanta or NSA's [National Security Agency's] knowledge about hackers that attacked Sony Pictures.

I guess I want to be real clear: are DOD elements looping in DHS to ensure civilian cybersecurity equities are considered before or after the fact?

General SHWEDO. So I will tell you, sir, you know, as we are going through pathfinders, et cetera, we are very cognizant of all the laws, and that is why you will hear Mr. Rapuano say we go through DHS. As it stands right now, we follow to the letter of the law, and that is much of the discussion that you hear between the two elements as we go forward.

We get requests for support from DHS, and then we turn it to over to lawyers on both sides of the street to make sure that we are following the piece. But any belief that somebody is going VFR direct[1] [visual flight rules, direct] to the Department of Defense is not what is happening. We work through DHS on all of our support.

Secretary RAPUANO. Just to add to that, DHS has the domestic protection mission. DOD is supporting DHS in the form of defense support to civil authorities through DHS's authorities. So, again, we are working very closely with DHS. DHS comes to us if they have got needs that are beyond what they can within their own capability sets employ, but if we were to employ them, it would be through DHS authorities.

Mr. RATCLIFFE. Okay. I very much appreciate that clarification. Thank you. I yield back.

Ms. STEFANIK. Mr. Richmond.

Mr. RICHMOND. Thank you.

Lieutenant General Shwedo, you answered pretty much my first question about collaboration between organizations, so let me focus for a moment on the funding aspect. With respect to securing civilian cyberspace, the role of civilian agencies in the military is well-defined. Congress has decided that outside of national emergencies, DHS, and not the armed services or the intelligence community, should lead these efforts.

So the question is about funding. Right now, DOD has an $8 billion budget for cyber, given DHS has basically $1 billion for critical infrastructure. Considering that 85 percent of critical infrastructure is privately owned, how do we balance that, and at what level would you say that a mission like that should be funded? And that is for the entire panel.

General SHWEDO. So, sir, the first piece is, you know, comparing the two budgets, first of all, Cyber Command is responsible for not only defensing—defensive actions here, but they also have a com-

[1] Air Force slang term concerning a pilot's ability to go straight to his destination; from aviation term meaning a simple flight plan.

batant command responsibility to ensure cyber warfare going on and the other piece. So that is one difference.

The other piece is, I think if you look at the responsibility, and we are still talking about how to fund some of these things, Mr. Rapuano will talk about it, but we have talked everything from—and this is part of the pathfinder, which has been a wonderful experience, is talking about the equivalent of a cyber Stafford Act and other things, because we are very cognizant of how funding in a bunch of different directions could get pretty bad.

The last part is, there is going to be a responsibility for a lot of these companies and other people that we have been talking about earlier to have their portion of cyber defense. For them to just put their hands up in the air and say we are not going to fund it anymore, I think, would also be a bill that we could not afford, but I will turn this over to Mr. Rapuano.

Secretary RAPUANO. I would just add that when you look at the DOD's budget, and the figure $8 billion is often used, the great majority of that funding does not go to U.S. Cyber Command. The great majority of that funding goes to development of weapon systems with cyber resilience and cybersecurity capabilities to the services.

Cyber Command, I believe, is under $500 million a year in terms of its funding, closer to $300 million, I believe. We can check that fact. But it is a very small percentage of the overall $8 billion, which is going into weapon systems and the Defense Information System and the CIO [Chief Information Officer].

Ms. MANFRA. From a DHS perspective, sir, we are a, you know—well, fairly new agency and we have been growing steadily. I would say that, you know, absolutely support the President's budget, appreciate the assistance through the omnibus and additional resources to assist us with the elections and helping with additional capabilities to civilian agencies.

But to help understand the scope, there are 99 civilian agencies that I am responsible for assisting with cybersecurity. There are—just in, you know, one sector alone, there are hundreds of thousands of companies that operate our water and wastewater treatment plants. So there is a massive scope and scale in what we are trying to secure.

We are very grateful to Congress for the authorities that we have been given, and we look forward to working with you to ensure that we have the capability and the capacity to deliver.

Mr. RICHMOND. Well, this is one of those golden moments. And, Lieutenant General, you kind of mentioned the Stafford Act. I am, you know, a survivor of Katrina and Rita. We don't hold the Stafford Act out to be the great example of anything, and I really wish this committee had—at least Homeland had jurisdiction over the Stafford Act so we could improve it.

But, Assistant Secretary Manfra, here is your opportunity to say, I think we have enough resources to protect the privately owned critical infrastructure; I think we don't. And what we don't want to happen—especially since my district is the first largest petrochemical district in the United States—what we don't want is Monday morning quarterback to say we didn't have the resources, we didn't have the support, we didn't get X, Y, and Z done.

So I guess my question is, as we head into budgeting and all the other stuff, do you think you have the resources to accomplish the mission that is so critical to everyone up here? So that is basically the question.

Ms. MANFRA. Sir, what I would say is that, as is demonstrated with the additional resources that you gave us for elections, we can do more with more.

Mr. RICHMOND. Thank you. And I yield back.

Ms. STEFANIK. Mr. Bacon.

Mr. BACON. Thank you all, all three for being here. I am grateful for your expertise and your hard work.

My first question is to General Shwedo, who I have worked with for quite a while. He has got a lot of experience in cyber warfare. And I would just like you to explain to our country and our citizens why this topic is so important that we don't have seams or overlapping, and if you could put it in the context of what would you anticipate on day one of a major cyberattack, say, from Russia or China.

This obviously would be a military directed attack at us, but will those targets be only towards military, or would you anticipate it being a wide array of targets in our country? If you could just elaborate what you would anticipate.

General SHWEDO. So I will just give an overview. We can definitely talk in detail in a closed session. But what we are seeing is, from both Russia and China, they prefer to stay below the level of the threshold of armed conflict. And you will find that we are seeing more and more when we see Ukraine and other countries, when you see power and other things start going out.

My concern is sometimes the citizenry is the soft underbelly, and I think that is kind of where you are going with the question, is we—and that is why this is so important, is we need to ensure that we shore up that, and that is part of the discussion we are having today as opposed to just throwing up our hands and saying we fight foreign wars.

We are not going to launch in and start taking over things in the United States. We are very cognizant to what DHS has to do, and that is why it is so important to make sure that we get it right when we go through these pathfinders, to make sure we get it right, that we get them the information and the support they need as it goes forward.

But I do believe your—the portion of your question is spot on. I do believe that it is going to be wide ranging. And I think if they get their way, just like the sons and daughters of Sun Tzu, they would prefer to not fight force on force. They would prefer to get their way below the level of the threshold of armed conflict, because the world has seen what happens when they go toe to toe with us, and that is not the preferred COA [course of action] they would like to go with.

Mr. BACON. So just to resummarize, it would be a military attack from their own cyber capabilities, but very likely the focus will be on areas covered by DHS. And this is why it is so important that we don't have these seams or overlapping things. It is very important that we have it right, because we know day one will not be a December 7 type attack. They will be going after our energy grid,

our financial sector, all those things that would create havoc. And so it requires significant cooperation between DOD and DHS to get this right.

And my next question will be to Ms. Manfra. We passed a bill earlier this year that gave DHS responsibility over industrial control systems. It is sitting in the Senate right now. How important is it to you and DHS that we get this out of the Senate and signed by the President?

Ms. MANFRA. Well, first of all, sir, I want to thank you all for recognizing the uniqueness of industrial control systems. These are the systems that really underpin most of our critical infrastructure. And DHS has had a unique role to play in industrial control systems, having some of the most recognized globally experts in our ICS–CERT [Industrial Control Systems Cyber Emergency Response Team]. So very much appreciate the acknowledgment that we need to have this leadership role and looking forward to continuing to work with the Senate and others to codify that.

Mr. BACON. We need to give a nudge over there, I think, get that signed—or voted on and sent over to the President.

My final question is this, and it gets back to really the focus of your-all's time here today. Do any of you see where we have overlapping responsibilities where it is creating problems? Do you need more delineation through legislation? Do you have any recommendations for us in that area? So do we have areas of overlap or do we have areas of seams that we need to do better on? Thank you.

Ms. MANFRA. Sir, I don't see any areas of overlap. We have definitely identified that there is a potential for seams and so we are working to address those, going back to starting at these national critical functions. And I know DOD is thinking about what is critical to their capability as well.

And so working together to ensure that we are bringing the full force of both of our authorities. I do believe that they are very complementary. I don't believe that they are duplicative or overlapping in any way. And so we are just going to continue to ensure that we can operationalize those authorities so that we can both do our missions.

Mr. BACON. Mr. Rapuano, anything to add?

Secretary RAPUANO. So as Secretary Manfra notes, we are in the process right now of looking at what our critical national functions are. And typically, because we looked at the homeland as a sanctuary traditionally over time and with the threat of cyber in particular, the homeland is no longer that sanctuary. We are looking at all of our dependencies as the Department of Defense and our ability to project power, where they are in critical infrastructure and how we can better ensure their resilience, so in the event of a conflict——

Ms. STEFANIK. Time is expired.

Secretary RAPUANO [continuing]. We will be able to leverage them. Thank you.

Mr. BACON. Thank you. I yield.

Ms. STEFANIK. Mrs. Demings, you are recognized for 5 minutes. Mrs. Demings, you are recognized for 5 minutes.

Mrs. DEMINGS. Thank you so much, Madam Chair. And thank you to our witnesses for being with us today.

This question is really for the entire panel, and I do appreciate the information that you shared with us thus far in this very critical area. And my question goes back to collaboration, cooperation. A question was asked earlier about resources, and I think we do better when we have the ability to share information and better work together.

So my question is, how are DHS and DOD working together on supply chain risk, especially in light of the growing overlap between the Defense Industrial Base and traditionally civilian sectors of U.S. critical infrastructure?

Ms. MANFRA. I can start, ma'am. This is actually one of our key areas of focus, given the exact point that you just made, that the many civilian agencies use many of the same companies that are in the Defense Industrial Base and that DOD uses. There is a series of actions, some of which we can talk about in the closed hearing as well, that we are ensuring that we are coordinating. So that we are using our authorities to drive better risk practices, both with the agencies that I have the directive authority under with civilian FISMA [Federal Information Security Management Act] agencies, as well as on the DOD side, but that we are also sharing information, and that we are coordinating and ensuring that if we are aware of a compromise of a vendor for one agency, that both of our agencies are aware of that and we can take coordinated action.

Mrs. DEMINGS. Thank you.

Secretary Rapuano.

Secretary RAPUANO. I thank you for the question. It is a very significant focus and concern, in terms of the supply chain and the dependency that we have on it for our weapon systems and communications capabilities.

We are focused in the interagency with DHS, but other key agencies, Commerce and others, in terms of identifying where the vulnerabilities are and how do we identify how we can restructure and better protect critical supply elements necessary for the economy and the military.

Mrs. DEMINGS. And General Shwedo.

General SHWEDO. Yes, ma'am. So this clearly falls under the information sharing piece, and we are aggressively looking for these back doors, et cetera. And as soon as we find one, we go back to the relationship with DHS, or dependent on who is the recipient of this back door, to ensure that we start sharing the information, because we understand that there's multiple actors in this realm and we are trying to get after it.

Mrs. DEMINGS. How would you say the White House is coordinating these efforts, and how are roles and responsibilities currently aligned?

Ms. MANFRA. The National Security Council is working through much of this. As Mr. Rapuano noted, there is OMB, the Office of Management and Budget. When you are thinking about Federal procurement policy, legal teams need to get together from Department of Justice, et cetera.

So this is a whole-of-government effort that is being managed by the White House. Then there are specific things that DHS and DOD are committing to do with each other because of our unique

authorities and oversight over the networks that we have the oversight on.

Mrs. DEMINGS. Secretary Rapuano, would you like to add anything to your original answer?

Secretary RAPUANO. I would just concur with Secretary Manfra that this is a whole-of-government focus, because there are a number of different agencies with authorities and responsibilities and expertise, and it has been working very closely, at least from my observation.

General SHWEDO. I would just end with it has to be a whole-of-government approach. We have got to make sure that we track it down in all aspects. So absolutely, that is where it has to come from, and it has to go down to the lowest levels.

Mrs. DEMINGS. And you feel like you are on target with reaching your mission and your goals in that area?

General SHWEDO. So, ma'am, you know, the supply chain challenge is incredibly hard. And this is one of those ones we cannot fall off the target. We have got to stay focused on this the entire time.

And I unfortunately hate to tell you we will never, quote, "get there." We are going to have to continually, because there are always going to be bad guys that are going to be shaking windows and shaking back doors, trying to get into our systems, weapon systems, any supply chain piece, commercial off-the-shelf. They are going to do anything that they can. Sons and daughters of Sun Tzu, they will go like water to the least defended place and try to place their back door there.

Mrs. DEMINGS. Thank you all.

And, Madam Chair, I yield back.

Ms. STEFANIK. Thank you, Mrs. Demings.

Mr. Scott.

Mr. SCOTT. Thank you, Madam Chair.

And, ma'am, when you mention the word "procurement" in this particular field, I imagine you could spend weeks in committee meetings on that, and we will be looking forward to your input on how we best handle procurement.

I want to mention one other thing before I get to my specific question. We have got people effectively doing the same job from different agencies. And my question gets back to compensation and employee benefits and managing a workforce that comes through different agencies. If you have got tremendous discrepancies in pay, that can lead to problems in the management of your team.

Is that an issue that you have been able to address or is that something that you are going to need legislative help with?

Ms. MANFRA. Sir, we actually have received legislative help on this in a bill passed a few years ago.

Mr. SCOTT. Okay.

Ms. MANFRA. We are working to create what we call the Cyber Talent Management System. We have been able to leverage some existing authorities, direct-hire authority, retention incentives, to reward those who have achieved certain certifications in difficult-to-retain positions, those types of things, that have really reduced our attrition rate.

The Cyber Talent Management System, I really believe once we get this in place, it will really just be a complete revolution in how you think about public service and civil service, and we are really excited to get that on board. And I am working with Suzette Kent, the Federal CIO, to think about how do we ensure that all civilian agencies have the ability to recruit and retain quality talent. And so that is also a big initiative. You will see some of that in the National Cyber Strategy as well, thinking about that workforce of the future.

Mr. SCOTT. It is certainly an area where in the private sector, they can make significantly more money, and they are truly public servants in doing the work that they are.

My question gets specifically to the National Guard. I know the Army Guard and the Air Guard have established cyber units to support U.S. Cyber Command. In what cases can these units support their home States under State authority or other States on a State-to-State basis?

And, General, that may be best for you. How do you expect——

General SHWEDO. Actually, I will defer to Mr. Rapuano. He is working on this issue right now.

Mr. SCOTT. Okay. That is fine. Perfect. Thank you.

Secretary RAPUANO. So as recently as the elections, we had a number of circumstances where State National Guard were supporting the State elections process with their cyber expertise and skills. As I noted in my statement, we are looking at the orientation and structuring of National Guard support to the civil side of the equation, and that would be with Federal assistance, in terms of a mission force capability.

But I think as you know, the National Guard, we go with the total force construct in the Department of Defense, which means that you want to have maximum flexibility to utilize all of your force structure to hit your priorities. And if you are segmenting significant chunks of it for particular missions for particular supported elements, you might lose that.

So we are balancing in the assessment what the gain/loss is associated with dedicating certain elements of the Guard to cyber domestic missions versus having them in reserve for military missions. So that is a work in progress.

General SHWEDO. All I would say just on the end is this is really where the come together with DHS, because we have to have that whole-of-government approach before we throw too many National Guard members. DHS may be having support teams in there, so that is going to be part of the calculus in covering down on all of our bets to a cyber incident. So those are some of the conversations.

The last part, we are learning a lot as it goes forward with—just in one scenario, Mr. Rapuano had to sign a waiver to a policy to allow National Guardsmen to get TS/SCI [Top Secret/Sensitive Compartmented Information] information when, because they were in Guard status, they were limited to Secret. So, once again, we are learning a lot as we go through.

Mr. SCOTT. It is certainly a different type of mission, but I think that as time goes on, we are going to need to pull on the Guard just for the manpower that it is going to take to handle this mission. But thank you for what you do.

And, ma'am, I yield the 15 seconds.

Ms. STEFANIK. Mr. Larsen.

Mr. LARSEN. Thank you. Thanks for coming out.

I want to build on what Mr. Scott said, Mr. Rapuano. So in your testimony you say that you are responsible for leading this with the DHS, but are you the leader on this, looking at [section] 1653? Are we calling you when there is a question?

Secretary RAPUANO. Well, we work with the Joint Staff, and we work with——

Mr. LARSEN. Yeah, but you are doing the evaluation?

Secretary RAPUANO. Yes, yes.

Mr. LARSEN. Your name will be on——

Secretary RAPUANO. OSD [Office of the Secretary of Defense] policy is——

Mr. LARSEN. OSD policy. Then do you have a timeline for the evaluation?

Secretary RAPUANO. I don't. I can come back to you with a timeline.

Mr. LARSEN. You don't yet have an estimate of when you are going to get back to us?

Secretary RAPUANO. February.

Mr. LARSEN. February?

Secretary RAPUANO. Hot off the presses.

Mr. LARSEN. As part of the budget or separately?

Secretary RAPUANO. Separately.

Mr. LARSEN. Separately. Thank you.

And you mentioned a few criteria. Have you outlined the top criteria that you will use to evaluate the pilot program?

Secretary RAPUANO. Well, it is really a trade space analysis, looking at the various missions and capabilities, looking at the contingency planning, looking at the global synchronization/prioritization process that the Joint Staff runs, to best understand what the best return on investment is in terms of military capability invested against a certain range of problems and contingencies.

Mr. LARSEN. It sounds like a pretty broad—a fairly broad answer then still.

Secretary RAPUANO. Well, the study has—I have not plugged into the study in the last several weeks, so it has advanced beyond the last element of information I have from it.

Mr. LARSEN. Okay. So I think there are three States, including my State, that are in the pilot. If I am not mistaken, Washington—I am sorry, I am not mistaken that my State is Washington. Washington, Ohio, and Hawaii I think are the States.

Are you looking at different models for the CSTs [civil support teams] or are they all using the same model?

Secretary RAPUANO. I don't have that level of detail.

Mr. LARSEN. Thanks. And you are looking at cost, obviously, Federal portion versus State portion?

Secretary RAPUANO. Costing is part of the assessment.

Mr. LARSEN. Cost is part of the assessment.

And then as part of this, are you embedded with the CSTs, with the pilot projects in each State, or are you providing them an evaluation tool, they are getting back to you on that?

Secretary RAPUANO. I don't have that level of detail. I can come back to you with more of the framing in terms of how the study is being worked.

Mr. LARSEN. Could you do that, please?

Secretary RAPUANO. Yes.

[The information referred to can be found in the Appendix on page 69.]

Mr. LARSEN. It is essentially the gist of my questions. And if either General or Ms. Manfra have any comments with regards to the questions I have, that is fine. Great.

Thank you very much. I yield back.

Ms. STEFANIK. Mr. Hice.

Mr. HICE. Thank you, Madam Chair.

Secretary Manfra, let me begin with you. The cybersecurity strategy places some emphasis on the issue of supply chain risks, and that, of course, is a big concern to many of us, particularly in recent weeks, as there have been some reports of at least possible compromise in some microelectronics.

So I am curious what you all are doing, what you plan to do in this regard, specifically with Federal networks, but also with other stakeholders, national as well as global.

Ms. MANFRA. Thank you for the question, sir. We are addressing both the civilian network challenge as well as the national and, frankly, global issue.

On the Federal side, what I mentioned is both working, started with things like requiring the removal of Kaspersky last year when we directed that all agencies had to remove Kaspersky-branded products.

And what we have been doing since then is working with the intelligence community, the Department of Defense, GSA [General Services Administration], OMB, and working through what are the barriers to civilian agencies being able to best manage third-party risk.

It is a fairly monumental problem and it does require thinking about things like procurement and, which, you know, is challenging, but we are taking it on, and we are doing it with all agencies at the table.

On sort of in the complementary effort, one of the other National Risk Management Center initiatives is actually about supply chain specifically. So we have an entire initiative. We stood up a supply chain task force with our partners in the IT and the communications industry. Every major player that has a role in delivering technology both to the government and to the broader citizenry in our country and, frankly, globally.

And we are working through both to get their perspective on what the Federal government could be doing better, but also how can we make the ecosystem more secure so we are not so dependent on technology that is developed and delivered from countries that we are not okay with the laws that they have in place. It is a very challenging problem, but I think we have the right mechanisms in place.

Mr. HICE. So you are pleased with the direction things are going?

Ms. MANFRA. I am absolutely pleased. I always wish that you could revise procurement policy a little bit faster, but it is a process that we have to go through.

Mr. HICE. Mr. Rapuano, would you like to respond to that as well?

Secretary RAPUANO. Just very quickly. We are very focused on the vulnerabilities with regard to supply chain. We have concerns about the DODIN, the DOD information system; defense critical assets, in terms of looking very closely at potential vulnerabilities in the supply chain; and the Defense Industrial Base, in terms of the contract relationships. What are the requirements? How do we reduce the risk associated with contaminated supply, essentially.

Mr. HICE. Are you likewise satisfied with the direction we are going to have an appropriate defense?

Secretary RAPUANO. We have a lot of time and effort focused on it right now. It is a big challenge.

Mr. HICE. It is.

Okay. Madam Chair, I see the clock says I am expired. I don't know if that is accurate.

Ms. STEFANIK. You have 1 minute, 30 seconds.

Mr. HICE. Okay.

Ms. STEFANIK. Actually, it reset, so I will give you 30 more seconds, Jody.

Mr. HICE. Okay. Well, 30 more seconds isn't going to give me time to go into another question. But General, let me just ask you your perspective on the supply chain issue.

General SHWEDO. Sir, as said, this is a huge problem, and the bottom line is this is where the info sharing is so powerful. And we need to make sure that we get it rapidly to all the affected players. And that is one of the strengths of this exercise we are going through right now, because in the past, on our side we weren't always able to share it as well as we are right now. So yes, it is a much better future, but we have got a lot of work to do, sir.

Mr. HICE. Well, I am pleased to hear that. And, again, thank you for the work that each of you are doing. Obviously, this is an issue that impacts every agency and every department across the board, and at the heart of it is the defense and national security issues. So thank you for what you are doing in that regard.

And thank you, Madam Chair. I yield back.

Ms. STEFANIK. Thank you, Mr. Hice. Sorry about the time, but glad you got your questions in.

Ms. Jackson Lee, you are recognized for 5 minutes.

Ms. JACKSON LEE. Thank you to the Chair and multiple Chairs and multiple Ranking Members. Thank you to the panel that has made this presentation for us.

I am not eager to engage in hyperbole, but I do think that a potential cyberattack is something that we all should be concerned about as much as it would be pervasive enough to cross all of the elements of which we would be concerned, whether it deals with the question of war and peace, whether it is a domestic internal action, or whether or not it happens to impact the Nation's electric grid, water and sewage, the normal functions, transportation. It is an amazing reach that we have that I think this hearing is extremely important.

And I do think it is important to raise the question regarding the creation of the cyber defense, and to start off with my first question, which I think has been asked, but I would like to hear how effective the collaboration is with the cyber responsibilities of DHS and those of DOD. So we have DHS, we have DOD, and if you could just take a quick moment. Do you think it is fully integrated, it is parallel, that the distinctive duties are clear, the commands are clear, the working relationships could be better, or they are growing? I would be interested in that, Secretaries, and then to our Lieutenant General.

Ms. MANFRA. Ma'am, thank you for the question. From my perspective, I think we have come a very, very long way. And while there is absolutely room to continue to grow, I am very confident that we are on the right path.

As I briefly mentioned before, our approach is really about bringing the policy personnel, the legal teams, and the operators in the room together and thinking about what is it we need to accomplish our missions and how can we use our complementary authorities and capabilities to best do that. And I think that is the right approach.

We have already realized a great deal, whether that is on elections or in other spaces. There is definitely room to continue to integrate our teams and we are setting the stage to make that happen, but I think we have demonstrated that this can work in real-world scenarios, and I am very satisfied with the track that we are on.

Ms. JACKSON LEE. Thank you.

Secretary RAPUANO. I would agree with every point that Secretary Manfra made. We are looking at and moving out on integrating the policies, plans, and the implementation at the operational level.

As noted throughout this testimony, there are a lot of challenges in this space. There are a lot of cross-cutting equities within the government and between the government and the private sector. That is what we are focusing on and prioritizing amongst them and then really focusing our efforts at the highest priorities.

Ms. JACKSON LEE. General.

General SHWEDO. Yes, ma'am. I would just follow up with the good thing about what we are going through right now is it is not theoretical. We are actually going through real-world scenarios and we are seeing results, not just at the operational, but at the tactical level.

Whenever you see a Kaspersky or election manipulation, et cetera—and we will talk more about this when we go to the closed door—we are seeing at the lowest levels this information is getting where it needs to be and we are seeing results of what happens when the information gets there.

So we have got more work to do on where we get the relationship so we can be faster, because in the world of cyber it is all about speed, but I would say we are on a good path right now.

Ms. JACKSON LEE. In your next answer, you might mention—when you said "speed," I spent a day with Aspen Institute dealing with cybersecurity, and quantum was a very major aspect of it and how fast it is.

So let me ask this question very quickly, if the Chair would indulge me. First of all, I introduced H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act, and it passed the House. And it is to create a safe place for the private sector to feel safe enough or secure enough to submit to the government its vulnerabilities, since we know they have 85 percent or more of our cyber in the hands of the private sector.

So I appreciate as I ask this question if you would incorporate the concept of zero day possibilities, but working with the private sector, but specifically I want to ask about the WannaCry and NotPetya attacks as examples of disruptive cyber events that may have—or that had far-reaching implications. The impact of these type attacks were felt most acutely abroad, with much of the U.S. cyber infrastructure not seeing the full effect of these attacks.

But can you give examples of some of the far-reaching consequences for WannaCry and NotPetya to the United States, and what are some of the more pressing issues regarding Russia interference in the recent Federal election? If you could do that, incorporated with the potential of fast quantum technology and how we should be looking at that in terms of our defense. Secretary.

Ms. STEFANIK. We will have to take those answers for the record. The time is expired.

[The information referred to can be found in the Appendix on page 69.]

Ms. STEFANIK. We will now move to the closed session in Rayburn 2212 immediately and get through as much of that as possible before they call votes.

Thank you very much to the witnesses.

[Whereupon, at 4:30 p.m., the subcommittee proceeded in closed session.]

A P P E N D I X

NOVEMBER 14, 2018

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

NOVEMBER 14, 2018

Opening Statement
Chairwoman Elise M. Stefanik
Emerging Threats and Capabilities Subcommittee
Interagency Cyber Cooperation: Roles, Responsibilities and Authorities of DoD & DHS
November 14, 2018

The subcommittee will come to order.

Welcome to this joint hearing of the Armed Services Subcommittee on Emerging Threats and Capabilities with the Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection. Today we will examine interagency cyber cooperation and the roles, responsibilities, and authorities of the Department of Homeland Security and the Department of Defense. Holding this joint hearing has been a priority for subcommittee for the past few months and we are pleased that it has come together today. This is a timely opportunity to hear about recent interagency coordination efforts and the status of related FY2019 NDAA provisions.

This is a critically important topic that will shape our oversight going forward as we consider the long-term policy frameworks needed for the United States cyber enterprise. Our committee, and ETC in particular, has performed significant oversight of the cyber organization, operations, and mission force development within the Department of Defense. With this joint hearing, we can now take a broader focus on the cyber organization and capabilities within the entire United States government.

Cyber threats posed by both state and non-state adversaries continue to grow and evolve at a rapid pace.

These threats are not just to our military weapons and systems, but also to our nation's critical infrastructures. Attacks against the electric grid, the financial sector or our healthcare system could have profound impacts on our daily way of life and economic security. As we have seen in recent years, cyber attacks, such as WannaCry ransomware, can have significant adverse economic impacts, and bring the private sector and government services to a stand-still. And since the average response time to detect a cyber-attack is measured in months, not minutes or hours, we must improve our abilities to detect and respond to malicious cyber activity.

This year, three important cyber strategies were released by the White House, the Department of Defense, and the Department of Homeland Security. These strategies all recognize the importance of a whole-of-government approach to addressing the challenges posed by securing our Nation in cyberspace. They will be an important step in building a cohesive U.S. cyber enterprise.

And while this hearing isn't solely about election security, it affords us the timely opportunity to hear about the significant interagency efforts recently aimed at ensuring the security of our 2018 midterms elections. Protecting the elections required a broad approach led by the Department of Homeland Security that included contributions from the Department of Defense and many other partners.

Our subcommittee, in collaboration with the Homeland Security committee, has been active in addressing the issue of improving cooperation between the two Departments. In this year's fiscal year 2019 National Defense Authorization Act, we established a pilot program that allows the Department of Defense to provide technical cybersecurity personnel to the Department of Homeland Security in order to enhance security and resiliency of critical infrastructure. I look forward to hearing the status of this pilot program today.

Also in this year's NDAA, we created a National Security Artificial Intelligence commission that will be important in identifying the impact AI will have in the cyber domain.

As our adversaries continue to improve at increasing speeds, we must similarly grow our abilities to defend against these threats. I believe that we will only be successful if the United States can leverage the capabilities and authorities of all its departments and agencies in a united approach. We must reduce wasted resources on overlapping and duplicative efforts in government to make sure that we are using our cyber defense resources sensibly.

Both agencies here today have made great strides in building their cyber capabilities over the last few years. To build upon that progress, I firmly believe we need to continue to work to build interagency partnerships to ensure a whole-of-government approach to countering the growing cyber threat.

Let me welcome our witnesses today:

- Ms. Jeanette Manfra, Assistant Secretary for the Office of Cybersecurity and Communications at the Department of Homeland Security
- Mr. Kenneth Rapuano, Assistant Secretary of Defense for Homeland Defense & Global Security and Principal Cyber Advisor at the Department of Defense

And –

- Lt. Gen. Bradford Shwedo, Director for Command, Control, Communications and Computers /Cyber and Chief Information Officer at the Joint Chiefs of Staff.

We look forward to your testimony.

Before I turn to my friend and Ranking Member Jim Langevin of Rhode Island for his opening comments, I would like to take a moment to thank him for his hard work and dedication over the past two years of the 115th Congress. I think we have done great things together, Jim, across all areas of our subcommittee jurisdiction. I truly look forward to working together in the next Congress and continuing the strong collaborative and bipartisan tradition of the Armed Services Committee, and this subcommittee in particular.

I'd like to welcome Chairman John Ratcliffe of Texas from the Cybersecurity and Infrastructure Protection Subcommittee of the Homeland Security Committee to today's hearing

I'd also like to welcome Ranking Member Cedric Richmond of Louisiana to today's hearing.

Immediately following the conclusion of this open hearing, the members will transition to Rayburn 2212 for a closed, classified briefing from our witnesses.

Without objection, the witnesses' prepared statements will be made part of the record. I ask the witnesses please keep your remarks to no more than 5 minutes.

Ms. Manfra, we will begin with you.

SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

WASHINGTON OFFICE:
2160 Rayburn House Office Building
Washington, DC 20515
(202) 225-3816

DISTRICT OFFICE:
1919 SMITH STREET, SUITE 1180
THE GEORGE "MICKEY" LELAND FEDERAL BUILDING
HOUSTON, TX 77002
(713) 655-0050

ACRES HOME OFFICE:
6719 WEST MONTGOMERY, SUITE 204
HOUSTON, TX 77019
(713) 691-4882

HEIGHTS OFFICE:
420 WEST 19TH STREET
HOUSTON, TX 77008
(713) 861-4070

FIFTH WARD OFFICE:
4300 LYONS AVENUE, SUITE 200
HOUSTON, TX 77020
(713) 227-7740

Congress of the United States
House of Representatives
Washington, DC 20515

COMMITTEES:
JUDICIARY
SUBCOMMITTEES:
COURTS, INTELLECTUAL PROPERTY AND THE INTERNET
IMMIGRATION AND BORDER SECURITY

HOMELAND SECURITY
SUBCOMMITTEES
RANKING MEMBER
BORDER AND MARITIME SECURITY
TRANSPORTATION SECURITY

SENIOR WHIP
DEMOCRATIC CAUCUS



Congresswoman Jackson Lee

Statement
Joint Hearing of the
Subcommittee on Cybersecurity & Infrastructure Protection
and House Armed Services Committee Subcommittee on
Emerging Threats and Capabilities Joint Hearing

"Interagency Cyber Cooperation: Roles, Responsibilities and Authorities of the Department of Defense & the Department of Homeland Security"

November 14, 2018

- Chairman John Ratcliffe and Ranking Member Cedric Richmond, of the Homeland Security Committee's Subcommittee on Cybersecurity & Infrastructure Protection thank you for working with Chairwoman Elise Stefanik and Ranking Member James Langevin of the Armed Services Subcommittee on Emerging Threats and Capabilities to make today's hearing on "Interagency Cyber Cooperation: Roles, Responsibilities and Authorities of the Department of Defense & the Department of Homeland Security" possible.

- I look forward to the testimony of today's witnesses:
    - Ms. Jeanette Manfra, Assistant Secretary for the Office of Cybersecurity and Communications (CS&C), Department of Homeland Security;
    - Mr. Kenneth Rapuano, ASD for Homeland Defense & Global Security and Principal Cyber Advisor, Department of Defense; and
    - Lt. Gen. Bradford J. "B.J." Shwedo, Director for Command, Control, Communications and Computers /Cyber, Chief Information Officer, Joint Chiefs of Staff.

- The purpose of this hearing is to explore the discrete cybersecurity missions of Department of Defense (DOD) and the Department of Homeland Security (DHS).

- The Cybersecurity Act of 2015 makes clear that DHS, through the NCCIC, is the "Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities."

- The Cybersecurity Act is the most significant Federal cybersecurity law to date, and culminated years of negotiation between civil libertarians, intelligence, defense, national security, criminal justice, and industry stakeholders.

- The Department of Homeland Security, through the National Protection and Programs Directorate (NPPD), plays a central role in the federal government's cybersecurity apparatus and in coordinating federal efforts to secure critical infrastructure.

- DHS is charged with coordinating agency efforts to secure the (dot).gov domain, while also serving as the hub for cybersecurity information sharing between and among the private sector and federal government.

- As Ranking Member of the Judiciary Subcommittee on Crime, Terrorism, Homeland Security and Investigations and a senior member of the Committee on Homeland Security, I am a strong believer in the legislative process as the best path for addressing the most complex issues of the digital communication age.

- The Cybersecurity Act followed a series of controversial cybersecurity proposals that drew strong protest from privacy advocates.

- Among the most contentious aspects of those proposals were provisions that would have allowed private companies to share data on cyber threats – which, unless narrowly defined, could include personal information – directly with agencies involved in military or law enforcement operations such as the NSA or the FBI, thus granting them sweeping permission to surveil individual citizens.

- To address these concerns, Congress settled on DHS as the proper steward for such potentially sensitive information.

- Careful work was done by members of this Committee through the drafting of legislation and the introduction of amendments during the markup process.

- While the issue is settled from a statutory perspective, efforts to re-litigate the appropriate home for civilian cybersecurity activities continue to resurface.

- Concerns about DOD mission creep were re-ignited after the 2016 Presidential campaign season when then-candidate Trump made a number of comments suggesting he would give DOD broader authorities with respect to U.S. critical infrastructure, including by promising to direct the Joint Chiefs to develop "a comprehensive plan to protect America's vital infrastructure from cyberattacks, and all other form of attacks." Such a redistribution of power would disturb DHS' established role as

the civilian lead for cyber information sharing and incident response.

- There were also concerns early in this Administration about a potential executive order that would give DOD an outsized role in civilian cybersecurity.

- Although these concerns were never fully realized, it is important to note that incremental expansions in DOD's cyber posture, such as those described in a new DOD Cyber Strategy issued in September 2018 replacing a more tempered Obama-era strategy, could upset the current balance and undermine privacy and civil liberties.

- This Administration did take a major step in 2017, when USCYBERCOM, created in 2009, was elevated to Cyber Command (USCYBERCOM).

- CYBERCOMMAND is one of ten unified commands of the United States Department of Defense.

- CYBERCOMMAND unifies the direction of DoD cyberspace operations, strengthens DoD cyberspace capabilities, and integrates and bolsters DoD's cyber expertise.

- There are significant cybersecurity challenges facing our nation in the form of Quantum Computing and Artificial Intelligence, which would expand the capability of computing in ways that present significant opportunities and perilous security risks for both homeland cybersecurity and national defense.

- On November 8, 2018, I attended the Aspen Institute 3rd Annual Aspen Cyber Summit, which focused much of the day on candid conversations intended to bridge the gap between policy-makers and technologists who share an interest in strengthening the security of computing technology and networks.

- This was an important and unique opportunity to speak one-on-one with some of the nation's best and brightest minds and influencers in the area of cybersecurity and what the future may hold.

- My focus on cybersecurity as a member of Congress has been expressed in serious legislative efforts to affect how civilian and military computing security is addressed.

- Earlier this Congress, I introduced H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act, which was passed by the full Homeland Security Committee.

- H.R. 3202 requires the Secretary of Homeland Security to submit a report on the policies and procedures developed for coordinating cyber vulnerability disclosures.

- The report will include an annex with information on instances in which cyber security vulnerability disclosure policies and procedures were used to disclose details on identified weaknesses in computing systems that or digital devices at risk.

- The report will provide information on the degree to which the information provided by DHS was used by industry and other stakeholders.

- The reason that I worked to bring this bill before the committee is the problem often referred to as a "Zero Day Event," which describes the situation that network security professionals may find themselves when a previously unknown error in computing code is exploited by a cybercriminal or terrorist.

- I am pleased that the Committee on Homeland Security passed H.R. 3202 to address the need to support information sharing regarding threats to computing networks.

- The full House passed H.R. 3202 and it is now before the Senate.

- In the first few weeks of the 115th Congress I introduced a number of measures on the topic of cybersecurity to address gaps in our nation's cyber defensive posture:

    - SCOUTS Act – H.R. 940;
    - CAPITALS Act –H.R. 54;
    - SAFETI Act – H.R. 950;
    - Terrorism Prevention and Critical Infrastructure – H.R. 945; and
    - Cybersecurity and Federal Workforce Enhancement Act – H.R. 935.

- H.R. 940, the "Securing Communications of Utilities from Terrorist Threats" or the "SCOUTS Act," directs the Secretary of Homeland Security, in coordination with the sector-specific agencies, to work with critical infrastructure owners and operators and State, local, tribal, and territorial entities to seek voluntary participation on ways that DHS can best defend against and recover from terrorist attacks that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof.

- H.R. 940, is relevant to today's hearing because it addresses the need for a two-way communication process that enables private sector participants in information sharing arrangements with DHS to communicate their views on the effectiveness of the information provided; the method of information sharing; and their particular needs as time passes.

- Specifically, the bill establishes voluntary listening opportunities for sector specific entities to communicate their challenges regarding cybersecurity, including what needs they may have for critical infrastructure protection; and how DHS is helping or not helping to meet those needs.

- The Society of Maintenance and Reliability Professionals have

endorsed H.R. 940, and input on the legislation included the Edison Electric Institute, an electric utility association.

- H.R.54, the Department of Homeland Security's Cybersecurity Asset Protection of Infrastructure under Terrorist Attack Logistical Structure or CAPITALS Act, which directs the Department of Homeland Security (DHS) to produce a report to Congress regarding the feasibility of establishing a DHS Civilian Cyber Defense National Resource.

- H.R. 950, requires a report and assessment regarding Department of Homeland Security's response to terrorist threats to Federal elections.

- The Comptroller General of the United States is directed to conduct an assessment of the effectiveness of Department of Homeland Security actions to protect election systems from cyber-attacks and to make recommendations for improvements to the actions taken by DHS if determined appropriate.

- H.R. 935, the "Cybersecurity and Federal Workforce Enhancement Act" identifies and trains people already in the workforce who can obtain the skills to address our nation's deficit in the number of workers and positions available for those with needed skills.

- H.R. 940, the "Securing Communications of Utilities from Terrorist Threats" or the "SCOUTS Act," is relevant to today's hearing because this bill focuses on the communications sent by DHS to sector specific entities and the ability of these entities to communicate to the agencies their perspective on the usefulness of the information; the form of communication that would be most helpful; and requires a report to Congress by DHS on the views of critical infrastructure owners and operators on the information sharing process related to cybersecurity.

- Each of these bills will build upon an aggressive approach for

securing cyber technology to manage critical infrastructure, chemical facilities, and port operations, ranging from communication and navigation to engineering, safety, and pipelines, that are critical to protect our nation's interest.

- Over the past year, Russian actors' targeted U.S. election infrastructure, hackers escalated efforts to breach the domestic energy sector, and WannaCry and NotPetya ransomware wreaked havoc on public and private infrastructure around the world.

- According to Symantec, a leading provider of cybersecurity solutions, said that "The world of cyber espionage experienced a notable shift towards more overt activity, designed to destabilize and disrupt targeted organizations and countries."

- As cyber threats continue to evolve and become more sophisticated, so must U.S. efforts to confront them.

- I look forward to the testimony of today's witnesses.

- Thank you,

Statement for the Record

Jeanette Manfra
Assistant Secretary
Office of Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security

FOR A HEARING ON

Interagency Cyber Cooperation:
Roles, Responsibilities and Authorities of the Department of Defense and Department of Homeland Security

BEFORE THE
SUBCOMMITTEE ON CYBERSECURITY
AND INFRASTRUCTURE PROTECTION OF THE HOUSE HOMELAND SECURITY COMMITTEE

&

THE SUBCOMMITTEE ON EMERGING THREATS OF THE HOUSE ARMED SERVICES COMMITTEE

Wednesday, November 14, 2018
Washington, DC

Chairman Ratcliffe, Chairman Stefanik, Ranking Member Richmond, Ranking Member Langevin, and members of the Committees, thank you for today's opportunity to testify regarding the Department of Homeland Security's (DHS) ongoing and collaborative efforts to strengthen the cybersecurity of our Nation's critical infrastructure. Safeguarding and securing cyberspace is a core homeland security mission, and DHS's National Protection and Programs Directorate (NPPD) leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure.

NPPD is responsible for assisting agencies with the protection of 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 from malicious cyber activity. We work to enhance cyber threat information sharing across the globe in order to help critical infrastructure entities and government agencies protect their cyber systems and quickly recover should such an attack occur. By bringing together all levels of government, the private sector, international partners, and the public, DHS protects against cybersecurity risks, improves our whole-of-government incident response capabilities, enhances information sharing of best practices and cyber threats, and strengthens resilience of our Nation's critical infrastructure.

Threat Assessment

Cybersecurity 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 cyber criminals, nation states and their proxies, increase the frequency and sophistication of malicious cyber activity. 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 democracy.

Global cyber incidents, such as the "WannaCry" ransomware incident attributed to North Korea and the "NotPetya" malware incident attributed to the Russian military in May and June 2017, respectively, are examples of malicious actors leveraging cyberspace to create disruptive effects and cause economic loss. These incidents exploited known vulnerabilities in software commonly used across the globe. Prior to these events, DHS had already taken actions to help protect networks from similar types of attacks. NPPD's National Cybersecurity and Communications Integration Center (NCCIC) publishes a list of known software vulnerabilities and pushes this information out to stakeholders on a routine basis. Additionally, through requested vulnerability scanning, we helped stakeholders identify vulnerabilities on their networks so they could be patched before incidents and attacks occurred. Recognizing that not all users are able to install patches immediately, we shared additional mitigation guidance to assist network defenders. As the incidents unfolded, we led the Federal Government's asset response efforts, working with our interagency partners, in providing situational awareness, information sharing, malware analysis, and technical assistance to affected government and critical infrastructure entities.

In a series of incidents since at least May of last year, working with U.S. and international partners, DHS and the Federal Bureau of Investigation (FBI) have identified Russian government actors targeting government entities and businesses in the energy, nuclear, water, aviation, and critical manufacturing sectors. Consistent with Presidential Policy Directive 41 and the National Cyber Incident Response Plan, DHS, FBI, and ODNI led coordination of the Federal Government's incident response. Support was also provided by the Department of Energy (DOE) and the Department of Defense (DOD), certain elements of the Intelligence Community, and the Nuclear Regulatory Commission.

DHS assesses that this campaign ultimately collected information pertaining to industrial control systems (ICS) with the intent to gain access to ICS environments, and in minimal instances did develop access to the ICS environments. The intrusions have been comprised of two distinct categories of victims: (1) staging and (2) intended targets. Through the Department's incident response actions, we identified activities by Russian government actors to target certain entities that then become pivot points, leveraging existing relationships between the initial victim and the intended targets to hide their activity, as part of a multi-stage intrusion campaign to gain access to networks of our Nation's critical infrastructure. Based on our analysis and observed indicators of compromise, DHS has confidence that this campaign is still ongoing, and threat actors are actively pursuing their ultimate long-term campaign objectives. DHS and FBI continue to conduct incident response related to this activity and have published a joint technical alert and hosted public webinars to enable network defenders to identify and take action to reduce exposure to this malicious activity.

As another example of specific threats, the U.S. Government has received information from multiple sources—including public and private sector cybersecurity research organizations and allies—that cyber actors are exploiting large numbers of network infrastructure devices (e.g., routers, switches, firewall, and network-based intrusion detection system devices) worldwide since 2015. Earlier this year, DHS, FBI, and the United Kingdom's National Cyber Security Centre published a publicly-available joint technical alert attributing this activity to Russian state-sponsored actors. Targets are primarily government and private-sector organizations, critical infrastructure providers, and Internet service providers supporting these sectors. Several days after publication of the alert, an industry partner notified DHS and FBI of related malicious cyber activity in which the actors redirected certain queries to their own infrastructure and obtained sensitive information, which included the configuration files of networked devices. Russian state-sponsored actors are using compromised routers to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations.

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. DHS and DOD recently 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 US 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.

Cybersecurity Priorities

DHS, our government partners, and the private sector are committed to a more strategic and unified approach as we work to improve our Nation's overall defensive posture against

malicious cyber activity. In February 2013, Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, recognized that only a more integrated approach to managing risk would enable the Nation to counter malicious cyber activity targeting our critical infrastructure. In May of this year, DHS published a Department-wide Cybersecurity Strategy, providing DHS with a strategic framework to execute our cybersecurity responsibilities during the next five years.

This Administration has leaned forward even further, prioritizing the protection and defense of our people and economy from the range of threats that exist today, including those emanating from cyberspace. In September the President released the National Cyber Strategy which recognizes that cyberspace has become foundational to our American way of life. Last year, the President signed Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This Executive Order set in motion a series of assessments and deliverables to enable the improvement of our defenses and lower our risk to cyber threats.

EO 13800 requires continued examination of how the Federal Government and industry work together to protect our Nation's critical infrastructure, prioritizing deeper, more collaborative public-private partnerships in threat assessment, detection, protection, and mitigation. In collaboration with civilian, defense, and intelligence agencies, we have worked to identify authorities and capabilities that agencies could employ, soliciting input from the private sector, and developed recommendations to support the cybersecurity efforts of those critical infrastructure entities at greatest risk of attacks that could result in catastrophic impacts. It is only through this collective defense model that we will be successful against this threat.

Additionally, under EO 13800, DHS and DOE, in consultation with ODNI, and state and local governments, assessed the potential scope and duration of a prolonged power outage associated with a significant cyber incident and the readiness to manage its consequences. DOE and DHS are focused on closing identified gaps in order to build on the already robust collaboration between government and industry on electricity sector cybersecurity. Continuing to enhance these partnerships is critical to enhancing cybersecurity preparedness and response capabilities, limiting the potential scope and duration of a significant cyber incident, and reducing impacts to the critical national economy, defense, and lifeline functions which the electric grid supports.

Department of Homeland Security's Cybersecurity Responsibilities

In accordance with the *Homeland Security Act of 2002*, as amended, the *National Cybersecurity Protection Act of 2014*, the *Federal Information Security Modernization Act of 2014*, the *Cybersecurity Act of 2015*, and Presidential Policy Directives 21 and 41, among other authorities and directives, DHS leads the Federal Government's efforts to enhance the cybersecurity and resilience of our Nation's critical infrastructure. As the next legislative step, we must ensure that NPPD is appropriately organized to address cybersecurity threats both now and in the future. Therefore, we urge the House to bring the Cybersecurity and Infrastructure Security Agency Act to the floor for final passage. This legislation would establish a cybersecurity agency at DHS, and realign NPPD to ensure it is focused on the core mission.

NPPD's NCCIC operates at the intersection of the private sector, state and local governments, federal departments and agencies, international partners, law enforcement, and intelligence and defense communities. The *Cybersecurity Information Sharing Act of 2015* established DHS as the Federal Government's central hub for the automated sharing of cyber threat indicators and defensive measures. The NCCIC's automated indicator sharing (AIS) capability allows the Federal Government and the private sector network defenders to share technical information at machine speed. The NCCIC also provides entities with information, technical assistance and guidance they can use to secure their networks, systems, assets, and information by reducing vulnerabilities and ensuring resilience to cyber incidents. DHS does this in a way that protects privacy and civil liberties.

NPPD's NCCIC provides a broad range of capabilities to assist private sector entities across all 16 sectors of critical infrastructure. In addition to information sharing and incident response, these capabilities include assessments and technical services that include recommended remediation and mitigation techniques that improve the cybersecurity posture of our Nation's critical infrastructure. Among other services, these include vulnerability scanning and testing, penetration testing, phishing assessments, and red teaming on operational technology that includes the industrial control systems that operate our Nation's critical infrastructure.

While DHS makes available to our Nation's critical infrastructure owners and operators unclassified and classified cyber threat information as well as a full range of technical assistance capabilities, DHS also closely coordinates with our federal partners, including Sector-Specific Agencies. For instance, the DOE is the Sector Specific Agency for the energy sector. DHS and DOE cooperate on a range of cybersecurity matters, particularly regarding information sharing, incident response, and research and development. NPPD's NCCIC works closely with DOE and the Energy Sector's Electricity Information Sharing and Analysis Center and Oil and Natural Gas Information Sharing and Analysis Center to share actionable information. We work closely with DOE to ensure we do not duplicate resources in areas such as incident response or information sharing, but also to ensure we leverage DOE's unique relationships and capabilities in the sector.

NPPD also funds work at the Idaho National Lab to enhance the cybersecurity of our Nation's industrial control systems that operate critical infrastructure, such as the electricity grid. This work includes a biannual conference with experts from across the industrial control systems cybersecurity community to ensure information and experience is shared across this community. In addition to assessments and sharing of technical cyber threat information, through Idaho National Lab, NPPD provides extensive hands-on training to the critical infrastructure owners and operators on protecting and securing industrial control systems from cyber-attacks and includes a red team/blue team exercise conducted within an actual control systems environment.

National Risk Management

We face an urgent, evolving crisis in cyberspace. Our adversaries' capabilities online are outpacing our stove-piped defenses. Working together with the private sector and our government partners, we are addressing this problem and taking collective action against

malicious cyber actors. Specifically, there is a need to enhance and promote the Department's cross-sector, cross-government coordination on critical infrastructure security and resilience.

We must improve our focus on examining the critical functions that drive our economy and facilitate national security. In other words, we need to continually advance our ability to organize and collaborate on risk strategies, planning, and solutions. For many years, DHS has worked closely with the private sector, but it has become clear that it must be a focal point for turning threat intelligence into joint action.

At the Department's first National Cybersecurity Summit this summer, in response to a clear demand signal and after extensive consultation with industry and government partners, Secretary Nielsen announced the rebranding of the Office of Cyber and Infrastructure Analysis as the National Risk Management Center (NRMC). Housed within DHS, the NRMC is the logical evolution of the ongoing improvements made over the last several years in information sharing and partnership building between the government and industry. The NRMC draws on existing resources and functions from across NPPD, the Department and our Federal and international partners to bring our risk management efforts to the next level of effectiveness.

The NRMC's mission is to enable analysts and planners, from both public and private sector, to jointly assess our country's cyber risks, plan to combat those risks and—most importantly—enable implementation of tailored solutions to protect our networks. The full expertise of the Federal Government should be brought to bear on these challenges.

Perhaps most importantly, the NRMC's core mission focuses on the systems or functions that cut across sectors. Ultimately, the NRMC will facilitate a partnership among and across government and industry that can provide a unified, collective approach to the defense that the nation needs to achieve superiority over our adversaries.

The NCCIC and National Infrastructure Coordination Center (NICC) will continue to carry out current operations, and the NRMC will enhance their efforts. The NRMC will support NCCIC and NICC operations by helping with prioritization and other needs, while also looking ahead to plan more strategically, and leveraging feedback from operations and other partners.

Conclusion

In the face of increasingly sophisticated threats, DHS employees lead efforts to defend our Nation's critical infrastructure from cyber threats. Our infrastructure environment today is complex and dynamic with interdependencies that add to the challenge of securing and making it more resilient. Clearly, we cannot do this unless we work together with our interagency partners, and use all available capabilities, people, and information. DHS remains committed to leading this effort while working hand in hand with our interagency partners to leverage every tool we have available. Further, as new threats emerge, we redouble our efforts. Expertise in cyber-physical risk assessments and cross-sector critical infrastructure interdependency evaluation is where NPPD brings unique experience and capabilities.

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

Jeanette Manfra

Jeanette Manfra serves as the National Protection and Programs Directorate (NPPD) Assistant Secretary for the Office of Cybersecurity and Communications (CS&C). Ms. Manfra leads the Department of Homeland Security (DHS) mission of strengthening the security and resilience of the nation's critical infrastructure.

Prior to this position, Ms. Manfra served as Acting Deputy Under Secretary for Cybersecurity and Director for Strategy, Policy, and Plans for the NPPD.

Previously, Ms. Manfra 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 Office of Cybersecurity and Communications, 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.

STATEMENT OF

MR. KENNETH RAPUANO

ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE

AND GLOBAL SECURITY

TESTIMONY BEFORE THE HOUSE ARMED SERVICES

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

AND THE HOUSE HOMELAND SECURITY SUBCOMMITTEE ON

CYBERSECURITY AND INFRASTRUCTURE PROTECTION

NOVEMBER 14, 2018

INTRODUCTION

Chairwoman Stefanik, Chairman Ratcliffe, Ranking Members Langevin and Richmond, and members of the committees, thank you for the opportunity to testify on interagency cyber cooperation between the Department of Defense (DoD) and the Department of Homeland Security (DHS). Last week's mid-term elections serve as a timely inflection point to review the close collaboration between our two Departments, and I appreciate the opportunity to discuss the sea change in our partnership. I would like first 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 for Fiscal Year 2019, which supports a range of military operations in cyberspace to disrupt, defeat, and deter malicious cyber activities.

THE THREAT

Before reviewing the Department's strategic posture for cyberspace, I would like to offer a few observations on the threat environment. As the National Defense Strategy and 2018 DoD Cyber Strategy make clear, the 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 infrastructure, and reduce our economic prosperity. In particular, we are engaged in a long-term competition with China and Russia. These states have expanded that competition to include persistent campaigns in and through cyberspace that are individually below the threshold of armed conflict, but that collectively pose long-term strategic risk to the Nation, as well as to our allies and 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.

STRATEGIC POSTURE

In September, the President released the new National Cyber Strategy, which highlights the growing threat that malicious cyber actors pose to our national security. The 2018 DoD Cyber Strategy commits the Department to fulfill its role in the National Cyber Strategy. Nested within the National Security and National Defense Strategies, and released shortly after the release of the 2018 DHS Cybersecurity Strategy, the 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. It normalizes the cyberspace domain, integrating cyberspace operations into military operations in the physical domains of air, land, sea, and space. It also makes clear that DoD's focus in cyberspace, like in other domains, is to "defend forward"—that is, to prevent or mitigate threats before they reach U.S. soil. This focus complements the DHS Cybersecurity Strategy's emphasis on domestic preparedness and risk management. Together, the DoD and DHS strategies form a national, mutually supporting approach to "defense in depth."

Specific to our collaboration with DHS, the 2018 DoD Cyber Strategy identifies three important roles for DoD in defending the homeland. First, by defending forward, DoD will seek to preempt, defeat, or deter malicious cyber activity targeting the United States that could cause a significant impact. This includes malicious cyber activity that falls below the use of force.

Second, DoD will strengthen the resilience of networks and systems that

contribute to current and future U.S. military advantages. Past strategies have taken a narrow view of what the Department must defend to ensure it is capable of performing its assigned missions. The evolving cyber threat and increasingly provocative activities of key competitors have demonstrated threats and vulnerabilities that extend beyond the DoD Information Network, and this threat must be addressed as a priority. Our interagency, international, and private sector partners will be key to implementing this pillar of the strategy to ensure that DoD can operate in a contested cyber environment.

Third, DoD has prioritized partnerships. DoD will identify the means by which to support its partners, but it also will seek to identify ways those partners can inform and enable DoD missions. For example, DoD will leverage its intelligence and operational capabilities to provide indications and warning of malicious cyber activity to other Federal partners and the private sector. But, for these partnerships to be effective, information and threat intelligence must flow back to DoD to inform the conduct of cyber operations. Timely feedback between our organizations will continuously improve the quality of the information exchange.

We are moving aggressively to implement the DoD Cyber Strategy. As directed by the National Defense Authorization Act for Fiscal Year 2018, the Department conducted a comprehensive review of its cyber posture and ability to execute the Strategy. The review included extensive background research, data collection, and expert interviews. This classified review identified that we must continue investments in our people, capabilities, and processes to meet fully the objectives set forth in the Strategy. Secretary Mattis and Deputy Secretary Shanahan are directly engaged in these efforts, and we have already identified, prioritized, and assigned leads to begin

implementing the Strategy across nine lines of effort.

TRANSLATING STRATEGY TO ACTION

With these new strategies in place, we have the right policy and guidance to support the defense of the United States in cyberspace. In response, DoD and DHS have worked together to establish a framework to drive domestic preparedness and critical infrastructure efforts. The 2018 mid-term elections are the first test of this expanded cooperation.

Secretary Mattis and Secretary Nielsen recently signed a joint memorandum that frames how DHS and DoD will secure and defend the homeland from cyber threats. This is a major step in fostering closer cooperation and marks a sea change in the level of collaboration between our Departments. 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 already underway. Yesterday, I joined my DHS and Joint Staff colleagues to sign the Joint DoD-DHS Cyber Protection and Defense Steering Group Charter. Established at the direction of Secretaries Mattis and Nielsen, this Steering Group will apply senior leadership energy to enhance U.S. Government readiness against cyber threats.

In this vein, DoD and DHS cooperated to ensure that all appropriate Federal government tools and resources were available to protect and defend the 2018 mid-term elections from foreign interference. As part of this effort, DoD provided standing approval for DoD personnel to support DHS cyber incident response activities in the event of a significant cyber incident impacting elections infrastructure that would have required a request for assistance from DHS. In preparation for a request for assistance from DHS, 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 should DHS request assistance from DOD.

The National Guard also played an important role in election support. Governors from several States used National Guard personnel in State status to support election cybersecurity in accordance with State law and policy. Examples of support included training exercises with local and State cyber officials and critical infrastructure partners, vulnerability and risk assessments, and information sharing. In addition, DoD authorized National Guard personnel in State active duty status, who already have security clearances, to access Top Secret Sensitive Compartmented Information to support securing the elections more effectively.

PATHFINDERS AND PLANS

Beyond elections, DoD is focused on how to improve collaboration with DHS in support of DHS's mission to assist the private sector with protecting critical infrastructure. Through a series of pathfinder initiatives, we are supporting DHS's efforts to enable

private sector entities to defend their networks by sharing relevant threat information. In turn, these pathfinders will enable DoD to partner with DHS in order to leverage private sector threat information to inform DoD cyberspace operations. We've begun our initial pathfinder effort through DHS with the financial sector and are working with DHS to establish a second pathfinder with the energy sector to build upon our existing information sharing efforts with the Department of Energy (DOE).

Separately, we are strengthening the Defense Industrial Base (DIB) Sector partnership to improve the security and resilience of DIB critical infrastructure. Specific lines of effort include: advancing information sharing, assessing and reforming DoD's approach to identification and risk management of DIB critical assets, and shielding future critical assets while they are still in development. This approach aligns with the National Defense Strategy guidance to enhance Joint Force lethality and reform Departmental procedures, and it complements our strategic approach on improving cybersecurity.

DoD is also coordinating with DHS's National Policy and Programs Division to establish a joint plan for future cyber incident response that required a request for assistance from DHS. At the tactical level, this effort has yielded a draft concept of operations that articulates how DoD's Cyber Mission Forces (CMF) would operate in support of DHS's Hunt and Incident Response Teams (HIRTs) in the event of a significant cyber incident. By identifying roles, responsibilities, and coordination mechanisms, we are jointly establishing a baseline for smooth, efficient, and effective interagency operations.

Lastly, I would be remiss if I didn't highlight the National Guard's contribution to

DoD and the Nation. The National Guard and Reserve are fully integrated into the CMF and will continue to grow. As a component of the total force, we continue to assess how best to leverage the unique position, relationships, and skill sets within the National Guard. We fully recognize the National Guard's two complementary roles as an integral part of the total force and as a State capability. Section 1653 of the National Defense Authorization Act for Fiscal Year 2019, which requires an assessment of the feasibility and advisability of establishing Cyber Civil Support Teams, provides an opportunity to review and refine the role of the National Guard. My team will lead this review with the Department of Homeland Security.

CONCLUSION

Thank you again for the opportunity to appear before you today. As you can see, the Department has undertaken extensive work with DHS to improve defense of the homeland and critical infrastructure, but there is much left to do. I look forward to working with Congress as we address these challenges facing the homeland, and I welcome your questions.

Kenneth P. Rapuano
Assistant Secretary of Defense for Homeland Defense and Global Security

Mr. Kenneth P. Rapuano is the Assistant Secretary of Defense for Homeland Defense and Global Security. Previously Mr. Rapuano was a Senior Vice President at the ANSER Corporation, and the Director of the Studies and Analysis Group which provided multi-disciplinary studies and operational analysis for a broad array of government clients in the national security, homeland security areas. Up until November of 2016, Mr. Rapuano Directed the Homeland Security Studies and Analysis Institute (HSSAI), a Federally Funded Research and Development Corporation (FFRDC) operated by ANSER, a mission oriented not-for-profit organization.

Prior to joining ANSER Mr. Rapuano was the Director of Advanced Systems at the MITRE Corporation. He was responsible for guiding crosscutting strategic national and homeland security mission initiatives, with particular focus on counterterrorism, intelligence, aviation security, crisis management/decision support, national preparedness, and CWMD.

Previously, Mr. Rapuano served at the White House as Deputy Homeland Security Advisor to President George W. Bush from 2004-2006. He was responsible for managing the development and implementation of homeland security policies among departments and agencies, chaired the Homeland Security Council Deputies Committee, and co-chaired the White House Counterterrorism Security Group. He left the White House in 2006 to volunteer for deployment as a Marine Corps officer to Afghanistan with a Joint Special Operations Task Force, establishing and directing a targeting fusion center tracking high-value terrorists and insurgents. He also served in Iraq in 2003, commanding the Joint Interrogations and Debriefing Center of the Iraq Survey Group established to conduct the mission of surveying and exploiting possible weapons of mass destruction activities across Iraq.

In 2003, Mr. Rapuano was appointed Deputy Under Secretary for Counter Terrorism at the Department of Energy, responsible for nuclear counter terrorism, homeland security, emergency response, and all related special access programs for DOE and the National Nuclear Security Administration. Previous to that, he was the National Security Advisor to the Secretary of Energy. Mr. Rapuano has also served as Special Assistant to the Assistant Secretary of Defense, International Security Policy. He served 21 years on active duty and in the reserves as a Marine Corps infantry officer and intelligence officer.

Mr. Rapuano has also served as a Distinguished Research Fellow at the National Defense University's Center for the Study of WMD, as a member of the Defense Science Board Task Force on the Role of DoD in Homeland Defense, the Pacific Northwest National Lab's National Security Advisory Committee, the FBI's Weapons of Mass Destruction Directorate Advisory Group, the DHS Quadrennial Homeland Security Review Advisory Committee, and the DHS Science and Technology Advisory Committee.

Mr. Rapuano received a bachelor's degree in Political Science from Middlebury College, a master's degree in National Security Studies from Georgetown University, and has attended the Marine Corps Air-Ground Task Force Intelligence Officer Course at the Navy and Marine Corps Intelligence School.

Lieutenant General Bradford J. "B.J." Shwedo

Lt. Gen. Bradford J. "B.J." Shwedo is the Director for Command, Control, Communications and Computers /Cyber, Chief Information Officer, Joint Staff, J6, the Pentagon, Washington, D.C. He develops C4 capabilities; conducts analysis and assessments; provides Joint and Combined Force C4 guidance, and evaluates C4 requirements, plans, programs and strategies for the Chairman of the Joint Chiefs of Staff.

General Shwedo graduated from the U.S. Air Force Academy in 1987, earning a Bachelor of Science in military history. Prior to his current assignment, he was the Chief, Information Dominance and Chief Information Officer for the Office of the Secretary of the Air Force at the Pentagon in Washington, D.C. As the SAF/CIO A6, General Shwedo led four directorates, supported 77,000 cyber operations and personnel across the globe with a portfolio valued at $17 billion. As the Chief Information Officer, he provided oversight of portfolio management, delivered enterprise architecture and enforced Freedom of Information Act and Privacy Act laws.

His staff assignments include Headquarters U.S. Air Force, Special Programs Division; Joint Chiefs of Staff, Special Activities Division; U.S. Cyber Command, Resource Integration Director; Intelligence Support to SAF/AQ; Executive Assistant to the Deputy Director of the Central Intelligence Agency; Director for Cyber Planning and Operations within the Office of the Secretary of Defense for Policy, and Director of Intelligence for the Air Combat Command. General Shwedo also led an intelligence team to Al Kharj, Saudi Arabia, in support of Operation Desert Shield/Storm. General Shwedo's commands include Detachment 2, 18th Intelligence Squadron, Osan Air Base, South Korea, and during the initiation of Operation Iraqi Freedom, he commanded the 566th Information Operations Squadron, which provided direct combat support through the National-Tactical Integration Program. General Shwedo's group and wing commands were within the 67th Network Warfare Wing, whose missions are to operate, manage and defend the Air Force's global networks. Throughout his tenure at the 67th NWW, this unit was in direct support of operations Enduring Freedom and Iraqi Freedom and the greater war on terror. General Shwedo also commanded the 25th Air Force at Joint Base San Antonio-Lackland, where he led 30,000 personnel in worldwide operations, delivering multisource intelligence, surveillance and reconnaissance products, applications, capabilities and resources.

EDUCATION

1987 Bachelor of Science in military history, U.S. Air Force Academy, Colorado Springs, Colo.
1992 Squadron Officer School, Maxwell Air Force Base, Ala.
1995 Master of Science of Strategic Intelligence, Joint Military Intelligence College, Washington, D.C.
1999 Master of Military Operational Art and Science, Air Command and Staff College, Maxwell AFB, Ala.
2000 Master of Airpower Art and Science, School of Advanced Airpower Studies, Maxwell AFB, Ala.
2004 Master of Arts National Security and Strategic Studies, United States Naval War College, Newport, R.I.
2008 Joint Forces Staff College, Joint and Combined Warfighting School, Norfolk, Va.

ASSIGNMENTS

June 1987 – June 1988, Assistant Football Coach, U.S. Air Force Academy, Colorado Springs, Colo.
June 1988 – March 1989, student, undergraduate pilot training, 82nd Flying Training Wing, Williams AFB, Ariz.
April 1989 – December 1989, student, intelligence training, 3486th Student Squadron, Goodfellow AFB, Texas
December 1989 – June 1992, Officer-in-Charge, Intelligence, 53rd Fighter Squadron, Bitburg AB, Germany, with deployed duties in support of Operation Desert Shield/Storm, Al Kharj AB, Saudi Arabia
July 1992 – May 1993, student, Defense Intelligence College, Bolling AFB, Washington, D.C.
May 1993 – June 1995, Threat Support Manager, 497th Intelligence Group, Falls Church, Va.

July 1995 – January 1997, Chief, Offensive Information Warfare, USAF/XOI, Special Programs Division, the Pentagon, Washington, D.C.
January 1997 – February 1998, Commander, Detachment 2, 18th Intelligence Squadron, Osan AB, South Korea
March 1998 – July 1998, Chief, Intelligence Systems, CADRE, Air University, Maxwell AFB, Ala.
August 1998 – July 1999, student, Air Command and Staff College, Maxwell AFB, Ala.
July 1999 – July 2000, student, School of Advanced Airpower Studies, Maxwell AFB, Ala.
July 2000 – July 2002, Operations Officer, Joint Chiefs of Staff, Special Activities Division, the Pentagon, Washington, D.C.
July 2002 – July 2003, Commander, 566th Information Operations Squadron, Buckley AFB, Colo.
August 2003 – June 2004, student, U.S. Naval War College, Newport Naval Station, Newport, R.I.
July 2004 – April 2005, Executive Assistant, Associate Director of Central Intelligence, Military Support, Headquarters CIA, Langley, Va.
April 2005– August 2006, Executive Assistant, Deputy Director—Central Intelligence Agency, Headquarters CIA, Langley, Va.
August 2006 – July 2008, Commander, 67th Network Warfare Group, Lackland AFB, Texas
July 2008 – July 2010, Commander, 67th Network Warfare Wing, Lackland AFB, Texas
August 2010 – November 2011, Director, Cyber Planning and Operations, Office of the Secretary of Defense, Policy, the Pentagon, Washington, D.C.
November 2011 – November 2013, Director of Intelligence, Headquarters Air Combat Command, Joint Base Langley-Eustis, Va.
November 2013 – July 2015, Director, Capability and Resource Integration (J8), U.S. Cyber Command, Fort Meade, Md.
August 2015 – June 2017, Commander, 25th Air Force, JB San Antonio-Lackland, Texas
June 2017 – June 2018, Chief of Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force, the Pentagon, Washington, D.C.
July 2018 — present, Director for Command, Control, Communications and Computers/Cyber, Chief Information Officer, Joint Staff, J6, the Pentagon, Washington, D.C.

SUMMARY OF JOINT ASSIGNMENTS
July 2000 - July 2002, Operations Officer, Joint Chiefs of Staff Special Activities Division, the Pentagon, Washington, D.C., as a major and lieutenant colonel
July 2004 - April 2005, Executive Assistant, Associate Director of Central Intelligence, Military Support, Headquarters CIA, Langley, Va., as a lieutenant colonel
April 2005 - August 2006, Executive Assistant, Deputy Director—Central Intelligence Agency, Headquarters CIA, Langley, Va., as a lieutenant colonel and colonel
August 2010 - November 2011, Director, Cyber Planning and Operations, Office of the Secretary of Defense, Policy, the Pentagon, Washington, D.C., as colonel and brigadier general
November 2013 - July 2015, Director, Capability and Resource Integration (J8), U.S. Cyber Command, Fort Meade, Md., as a brigadier general and major general.
July 2018 - present, Director for Command, Control, Communications and Computers/Cyber, Chief Information Officer, Joint Staff, J6, the Pentagon, Washington, D.C., as a lieutenant general

AWARDS AND DECORATIONS
Distinguished Service Medal
Defense Superior Service Medal with three oak leaf clusters
Legion of Merit with two oak leaf clusters
Defense Meritorious Service Medal
Meritorious Service Medal with three oak leaf clusters
Air Force Commendation Medal
Air Force Achievement Medal
Air Force Outstanding Unit Award
Air Force Organizational Excellence Award
National Defense Service Medal
Southwest Asia Service Medal

EFFECTIVE DATES OF PROMOTION
Second Lieutenant May 27, 1987
First Lieutenant May 27, 1989
Captain May 27, 1991
Major Aug. 1, 1998
Lieutenant Colonel March 1, 2002
Colonel March 1, 2006
Brigadier General Oct. 4, 2011
Major General March 1, 2015
Lieutenant General June 9, 2017

(Current as of August 2018)

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

NOVEMBER 14, 2018

RESPONSE TO QUESTION SUBMITTED BY MR. LANGEVIN

Secretary RAPUANO. Section 1653 of the National Defense Authorization Act for Fiscal Year 2019 requires an assessment of the feasibility and advisability of establishing State Cyber Civil Support Teams. My team, in collaboration with the Department of Homeland Security, is as of November 14, 2018, in the final stages of drafting that report and our intent is to deliver the final version to Congress in 2019. [Note: the final report was submitted to Congress in May 2019]. [See page 16.]

RESPONSE TO QUESTIONS SUBMITTED BY MR. LARSEN

Secretary RAPUANO. Washington, Ohio, and Hawaii National Guard personnel are participating in a pilot program to evaluate the utility of using National Guard (NG) cyber elements to support DOD missions. The NG pilot program employs select Army National Guard (ARNG) and Air National Guard (ANG) personnel to conduct DOD cyber training activities, both on and off the DOD Information Network (DODIN), with the incidental benefit of helping to protect defense critical infrastructure. DOD is cooperating with DHS on this program.

The pilot program currently underway differs significantly from the cyber civil support team (CST) concept as described in Section 1653 of the National Defense Authorization Act for Fiscal Year 2019. Most importantly, Section 1653 directs the Department to assess the feasibility and advisability of CSTs "organized . . . for the purpose of assisting State authorities," which would "[operate] principally under the command and control of the Chief Executive of the State." The cyber elements are participating in the NG pilot program for the purpose of accomplishing DOD training while providing incidental benefit to DOD mission assurance.

As of November 14, 2018, my team, in collaboration with the Department of Homeland Security, is in the final stages of drafting the report required by Section 1653, and our intent is to deliver the final version to Congress in 2019. The report will include cost assessments for several different models considered in the assessment, including the NG pilot program currently underway. [Note: the final report was submitted to Congress in May 2019]. [See page 26.]

RESPONSES TO QUESTIONS SUBMITTED BY MS. JACKSON LEE

Ms. MANFRA. [The information was not available at the time of printing.] [See page 29.]

Secretary RAPUANO. In May 2017, WannaCry infected hundreds of thousands of computers around the world, causing extensive damage. In June 2017, NotPetya encrypted and essentially ruined hard drives on thousands of Ukrainian computers, and then quickly spread well beyond Ukraine, causing billions of dollars in damages to businesses across Europe and as far away as the United States. Both WannaCry and NotPetya exploited a vulnerability in Windows that the Microsoft Corporation had patched weeks earlier.

We currently have no indication that any foreign adversary intended to manipulate votes or attack elections infrastructure in the 2018 U.S. midterm elections. However, we continue to see a pervasive messaging campaign by Russia to try to weaken and divide the United States.

Quantum computing has the potential to increase information processing speed exponentially. The addition of quantum computing affects both exploit and counter-exploit activities. The increased speed for an adversary to identify vulnerabilities and develop exploits could be matched by the speed in which security researchers identify exploitable products and notify the vendor, who would produce a software update or service patch. [See page 29.]

General SHWEDO. [The information is retained in the subcommittee files.] [See page 29.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

NOVEMBER 14, 2018

QUESTIONS SUBMITTED BY MS. STEFANIK

Ms. STEFANIK. Ms. Manfra, you are likely aware of the DOD's SharkSeer cybersecurity program, which orchestrates 23 commercial technologies to provide automated cyber defense for the DOD information network. It is my understanding that since becoming fully operational, SharkSeer has increased DOD detection rates by 886 percent and has discovered over 2 billion unique cyber events. I also understand that SharkSeer's automated means for detecting, analyzing and responding to nation-state cyber events has replaced the need for nearly 90 personnel to generate mitigations; now, only a few personnel are needed to approve automated work flows and interactive mitigations are executed in minutes rather than days—this means that DOD's security architecture is not only more secure, it's also more cost effective. In short, by any measurement, this a very successful program that could be replicated to protect a broader range of Federal networks.

Ms. Manfra, based on what I have described and what you know independently about the SharkSeer program, do you think there's an opportunity to leverage a similar architecture consisting of commercial-off-the-shelf technologies to protect civilian networks? Are you planning to collaborate with DOD on such an architecture?

Ms. MANFRA. [The information was not available at the time of printing.]

Ms. STEFANIK. What are DOD and DHS doing individually and collectively to manage risk associated with Internet of Things (IOT) and Operational Technology (OT) devices that are already deployed on government networks but lack sufficient security capability?

Ms. MANFRA. [The information was not available at the time of printing.]

Ms. STEFANIK. DHS has worked hard over the past few years, via the CDM program, to ensure that all internet-enabled devices that connect to a Federal civilian network can be identified and that such devices comply with network policies. I understand that DOD has developed a similar program referred to as Comply to Connect that is used by several of the service branches and DOD agencies, but is not fully rolled out enterprise-wide.

Please give me a sense as to how important it is that civilian networks be able to identify all of the devices, including IOT devices and Operational Technology devices, that seek to connect and that all such devices comply with network policies?

Ms. MANFRA. [The information was not available at the time of printing.]

Ms. STEFANIK. In September, the President signed an election security executive order that requires the Director of National Intelligence, in consultation with the heads of any other appropriate executive departments and agencies, to conduct an assessment on any election interference by a foreign government. This assessment is due 45 days after the election.

As an action from this hearing, we would like to request a copy of that assessment, when complete. If appropriate, the results of the assessment may also be included in the next quarterly cyber operations briefing.

Ms. MANFRA. [The information was not available at the time of printing.]

Ms. STEFANIK. In September, we had a briefing that discussed the DOD efforts to protect the 2018 midterm elections. In this closed setting, can you provide an update on the DOD and DHS efforts?

Ms. MANFRA. [The information was not available at the time of printing.]

Ms. STEFANIK. We have heard anecdotally that many of the current interagency cyber relationships have been ad hoc and are based on personal connections. Can you describe any frameworks that could be used to formalize these relationships and interactions? What level would these frameworks best be applied at?

Ms. MANFRA. [The information was not available at the time of printing.]

Ms. STEFANIK. The FY19 NDAA authorized a pilot program to provide Department of Defense technical personnel to the Department of Homeland Security to improve critical infrastructure cybersecurity. Can you give a status of this pilot program? What lessons have we already learned?

Ms. MANFRA. [The information was not available at the time of printing.]

Ms. STEFANIK. Where do you see the most value in expanding our current partnerships? Are there lessons learned from our interagency interactions that could be applied to strengthening our international partnerships?

Ms. MANFRA. [The information was not available at the time of printing.]

Ms. STEFANIK. Mr. Rapuano, you are likely aware of the DOD's SharkSeer cybersecurity program, which orchestrates 23 commercial technologies to provide automated cyber defense for the DOD information network. It is my understanding that since becoming fully operational, SharkSeer has increased DOD detection rates by 886 percent and has discovered over 2 billion unique cyber events. I also understand that SharkSeer's automated means for detecting, analyzing and responding to nation-state cyber events has replaced the need for nearly 90 personnel to generate mitigations; now, only a few personnel are needed to approve automated work flows and interactive mitigations are executed in minutes rather than days—this means that DOD's security architecture is not only more secure, it's also more cost effective. In short, by any measurement, this a very successful program that could be replicated to protect a broader range of Federal networks.

Mr. Rapuano, can you please share your general views on both the efficacy and the cost-effectiveness of the SharkSeer program? Has the DOD shared its learnings from the SharkSeer program with DHS as you coordinate on cybersecurity best practices?

Secretary RAPUANO. The National Security Agency (NSA) Sharkseer cybersecurity program integrates commercial-off-the-shelf technologies and threat intelligence to provide real-time detection, alerting, analysis, and mitigation of malware activity on national security systems and other government organization end point operations. In October 2016, NSA, in partnership with Defense Information Systems Agency (DISA), completed the worldwide deployment of Sharkseer perimeter defense capabilities at the ten DOD NIPRNet Internet Access Points. Section 1641 of the National Defense Authorization Act for Fiscal Year 2019 directs the transfer of the Sharkseer program from the NSA to DISA no later than March 1, 2019, for continued enterprise-wide operations. Sharkseer has been successful and cost effective to date.

Yes, DOD shares lessons learned from Sharkseer with DHS. Also, there are more than 800 registered users of the Sharkseer program, including DHS.

Ms. STEFANIK. Mr. Rapuano, in the 5 years since Edward Snowden's theft of classified information from the National Security Agency (NSA) became public, insider attacks—both malicious or accidental—have continued to embarrass and damage U.S. national security. One of the most recent insider attacks on a Federal agency involved a former NSA developer, Nghia Hoang Pho, who was found guilty of illegally exfiltrating a high volume of classified material, including sophisticated collection tools, between 2010 and 2015. According to former NSA Director Admiral Mike Rogers, Mr. Pho's actions "left the NSA with no choice but to abandon certain important initiatives, at great economic and operational cost." The human element in cybersecurity is a critical weakness and our efforts to date have not been sufficiently effective.

As we modernize our networks and move to a cloud environment with shared services, what are the Department of Defense and the Department of Homeland Security doing individually and together from a people, process, and technology perspective, to better manage risk from insiders in near real time while avoiding undue infringement upon the civil liberties of employees and contractors that support the government?

Secretary RAPUANO. In accordance with Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, dated October 7, 2011, DOD is implementing a strategic and layered approach to strengthen the mitigation of insider threats as it relates to technology, people, and processes, including the governance and management of efforts to counter insider threats.

First, with respect to technology, the Department is actively improving both user and network monitoring to mitigate insider threats more effectively. DOD organizations are employing user activity monitoring tools to monitor individual user activities on computers accessing and storing information and analyzing that activity. In addition, we are developing new tactics, techniques, and procedures that increase our ability to detect and report cyber insider threat events on information networks.

Second, with respect to people and processes, the insider threat must be addressed through understanding individuals and their interaction points with the Department. Thus, the Department is investing in the area of insider threat social and behavioral sciences (SBS) and considers this one of its strategic pillars. DOD researchers and social scientists have partnered with industrial and academic entities to conduct a number of SBS projects that will help understand the human behaviors of DOD personnel and contractors. Building on the outcome of these projects, we are modernizing and strengthening the hiring process and changing organizational processes and culture to encourage reporting (including identification for self-help). We

must be able to detect and manage at-risk employees to mitigate potential threats as early as possible.

Lastly, the Department takes a proactive approach to ensure appropriate protections of the privacy and civil liberties of DOD personnel and contractors. Accordingly, all insider threat and cyber security-related policy and procedures are reviewed and cleared by the DOD Privacy, Civil Liberties, and Transparency Division prior to release or implementation

Ms. STEFANIK. Mr. Rapuano, network traffic traversing both civilian and military IT systems is increasing exponentially in volume. As the overall volume increases, Gartner predicts that by 2019, 80% of that traffic will be encrypted. What are the DOD and DHS doing to ensure that appropriate network traffic, whether inbound, outbound, or moving laterally, can be de-crypted, inspected by the appropriate cybersecurity tools, and re-crypted?

Secretary RAPUANO. The Department of Defense is testing a number of ways that we might improve cybersecurity. The Defense Information Systems Agency is conducting a pilot program for inbound and outbound traffic designed to inspect encrypted traffic exiting and entering DOD enclaves at Internet Access Points (IAPs). We are learning a great deal from this pilot program and are making adjustments to enhance both performance and security based on what we are learning.

For lateral traffic, the Joint Regional Security Stack (JRSS) team—a network enclave security capability that monitors and inspects network traffic—is testing capabilities and working on solving significant performance challenges from the greater traffic volumes. Decisions on undertaking a pilot program and specific deployments are not yet finalized.

Ms. STEFANIK. What are DOD and DHS doing individually and collectively to manage risk associated with Internet of Things (IOT) and Operational Technology (OT) devices that are already deployed on government networks but lack sufficient security capability?

Secretary RAPUANO. DOD established cybersecurity policy in 2014, articulating security expectations for all DOD information technology (IT), including IOT and OT devices, as described in DOD Instruction 8500.01, Cybersecurity, and DOD Instruction 8510.01, the Risk Management Framework (RMF) for DOD Information Technology (IT). Through implementation of these policies, DOD is actively managing risk on systems already deployed on government networks, based on the criticality of the system. DOD will continue to update these policies to strengthen cybersecurity requirements for all end points, reducing the "weak links" in DOD networks and rewarding makers of OT and IOT devices for prioritizing security as much as cost and convenience.

The National Institute of Standards and Technology (NIST) is leading the development of commercial cybersecurity standards and national cybersecurity standards, and DOD is engaged in the development of both standards to ensure that DOD security requirements are integrated into future generations of products.

Ms. STEFANIK. DHS has worked hard over the past few years, via the CDM program, to ensure that all internet-enabled devices that connect to a Federal civilian network can be identified and that such devices comply with network policies. I understand that DOD has developed a similar program referred to as Comply to Connect that is used by several of the service branches and DOD agencies, but is not fully rolled out enterprise-wide.

What further resources does DOD need to ensure that Comply to Connect is utilized throughout the DOD network and what other impediments may exist?

Secretary RAPUANO. Comply-To-Connect (C2C) is a unified cybersecurity framework designed to reduce the Department's network attack surface through identification of all connected devices and enforcement of proper device configuration. C2C maintains continuous situational awareness of all device types connecting to the network and regulates access for devices with the greatest network exposure in accordance with DOD cybersecurity policies. DOD employs many of the cybersecurity toolsets used by the Continuous Diagnostics and Mitigation program.

The Department has programed funding to support the deployment of key elements of a C2C model starting in fiscal year (FY) 2020. Efforts in FY 2019 will lead to decisions about final product solutions, the number of cybersecurity frameworks the Department will support, and whether the Department will embrace a managed service construct to accelerate C2C deployment across all DOD networks. The Department's priorities for C2C were reflected in the President's FY20 Budget.

Ms. STEFANIK. In September, the President signed an election security executive order that requires the Director of National Intelligence, in consultation with the heads of any other appropriate executive departments and agencies, to conduct an assessment on any election interference by a foreign government. This assessment is due 45 days after the election.

As an action from this hearing, we would like to request a copy of that assessment, when complete. If appropriate, the results of the assessment may also be included in the next quarterly cyber operations briefing.

Secretary RAPUANO. On December 21, 2018, Director of National Intelligence Coats submitted the Intelligence Community's report on foreign interference in the 2018 U.S. midterm elections to the President and appropriate Executive departments and agencies, as directed by Section 1(a) of Executive Order 13848, dated September 12, 2018, Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election.

According to that report, "the Intelligence Community does not have intelligence reporting that indicates any compromise of our Nation's election infrastructure that would have prevented voting, changed vote counts, or disrupted the ability to tally votes. Russia and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns targeted at the United States to promote their strategic interests."

I defer the request for a copy of this report to the Office of the Director of National Intelligence.

Ms. STEFANIK. In September, we had a briefing that discussed the DOD efforts to protect the 2018 midterm elections. In this closed setting, can you provide an update on the DOD and DHS efforts?

Secretary RAPUANO. [The information is retained in the subcommittee files.]

Ms. STEFANIK. We have heard anecdotally that many of the current interagency cyber relationships have been ad hoc and are based on personal connections. Can you describe any frameworks that could be used to formalize these relationships and interactions? What level would these frameworks best be applied at?

Secretary RAPUANO. There are a number of means, both formal and informal, through which DOD interacts with other departments and agencies on matters related to cyberspace. In accordance with the Cybersecurity Information Sharing Act of 2015 and PPD–41 (United States Cyber Incident Coordination), DOD actively characterizes and assesses foreign cybersecurity threats and informs DHS of current and potential malicious cyberspace activity. DOD intelligence components may provide technical assistance to U.S. Government departments and agencies upon request through established relationships. In addition, the Secretary of Defense may approve providing DOD support to civil authorities in accordance with applicable law and policy. Further, the President has issued national policy that provides a framework for interagency consultation on certain types of cyber operations.

The Secretaries of Defense and Homeland Security signed a joint memorandum on defending the homeland from strategic cyber threats in October 2018. This memorandum frames how DHS and DOD will secure and defend the homeland. Specifically, it created a Cyber Protection and Defense (CPD) Steering Group (SG) to guide DOD–DHS cyber collaborative efforts. The CPD Steering Group recently approved its charter to formalize DOD–DHS collaborative efforts and prescribed next steps with the Department of the Treasury on engaging with the Financial Sector.

Section 1650 of the National Defense Authorization Act for Fiscal Year 2019 authorizes the Secretary of Defense to provide, assign, or detail up to 50 technical cybersecurity personnel to DHS on a non-reimbursable basis to enhance cybersecurity cooperation, collaboration, and unity of Government efforts. DOD is currently in the process of drafting and coordinating Section 1650 implementation requirements and identifying priority areas for collaboration between DOD and DHS personnel.

In addition, it is worth noting that, in 2008, National Security Presidential Directive–54/Homeland Security Presidential Directive–23 established the National Cyber Investigative Joint Task Force (NCI–JTF) as the focal point for all government agencies to coordinate, integrate, and share information related to all domestic cyber threat investigation. NCI–JTF is composed of more than 20 partnering agencies across law enforcement, the Intelligence Community, and DOD.

Ms. STEFANIK. The FY19 NDAA authorized a pilot program to provide Department of Defense technical personnel to the Department of Homeland Security to improve critical infrastructure cyber security. Can you give a status of this pilot program? What lessons have we already learned?

Secretary RAPUANO. Section 1650 of the National Defense Authorization Act for Fiscal Year 2019 authorizes the Secretary of Defense to provide, assign, or detail up to 50 technical cybersecurity personnel to the Department of Homeland Security (DHS) on a non-reimbursable basis to enhance cybersecurity cooperation, collaboration, and unity of Government efforts. Use of this authority requires the establishment of procedures relating to U.S. persons information.

DOD is currently in the process of coordinating Section 1650 implementation requirements, including procedures for the protection of U.S. person information, and identifying priority areas for collaboration between DOD and DHS personnel. We

are leveraging lessons learned from the placement of DOD personnel at DHS during the 2018 U.S. midterm elections as we develop the implementation procedures for Section 1650. For example, the protocols and processes employed by DOD personnel at the National Cybersecurity and Communications Integration Center (NCCIC) during the elections can be used by DOD personnel provided, assigned, or detailed to DHS pursuant to Section 1650. Similarly, our experience during the elections validated the utility of placing a DOD coordination element at the NCCIC when national-level crises arise.

Ms. STEFANIK. Where do you see the most value in expanding our current partnerships? Are there lessons learned from our interagency interactions that could be applied to strengthening our international partnerships?

Secretary RAPUANO. DOD strives to improve cooperative efforts with its partners but also sees value in expanding the ways in which those partners can inform and enable DOD missions. For example, DOD leverages its intelligence and operational capabilities to provide indications and warning of malicious cyber activity to other Federal partners and, as appropriate, the private sector. However, for these partnerships to be effective, DOD's partners also must provide information and threat intelligence to DOD to inform DOD's conduct of cyber operations.

The importance of mutual information sharing applies in the international context as well. Many of the United States' allies and partners possess advanced cyber capabilities that complement our own. The Department will seek to strengthen the capacity of these allies and partners, and, at the same time, increase DOD's ability to leverage its partners' unique skills, resources, capabilities, and perspectives. Information-sharing relationships with allies and partners will increase the effectiveness of combined cyber operations and enhance our collective cybersecurity posture.

Ms. STEFANIK. What are DOD and DHS doing individually and collectively to manage risk associated with Internet of Things (IOT) and Operational Technology (OT) devices that are already deployed on government networks but lack sufficient security capability?

General SHWEDO. [The information is retained in the subcommittee files.]

Ms. STEFANIK. In September, the President signed an election security executive order that requires the Director of National Intelligence, in consultation with the heads of any other appropriate executive departments and agencies, to conduct an assessment on any election interference by a foreign government. This assessment is due 45 days after the election.

As an action from this hearing, we would like to request a copy of that assessment, when complete. If appropriate, the results of the assessment may also be included in the next quarterly cyber operations briefing.

General SHWEDO. [The information is retained in the subcommittee files.]

Ms. STEFANIK. In September, we had a briefing that discussed the DOD efforts to protect the 2018 midterm elections. In this closed setting, can you provide an update on the DOD and DHS efforts?

General SHWEDO. [The information is retained in the subcommittee files.]

Ms. STEFANIK. We have heard anecdotally that many of the current interagency cyber relationships have been ad hoc and are based on personal connections. Can you describe any frameworks that could be used to formalize these relationships and interactions? What level would these frameworks best be applied at?

General SHWEDO. [The information is retained in the subcommittee files.]

Ms. STEFANIK. The FY19 NDAA authorized a pilot program to provide Department of Defense technical personnel to the Department of Homeland Security to improve critical infrastructure cyber security. Can you give a status of this pilot program? What lessons have we already learned?

General SHWEDO. [The information is retained in the subcommittee files.]

Ms. STEFANIK. Where do you see the most value in expanding our current partnerships? Are there lessons learned from our interagency interactions that could be applied to strengthening our international partnerships?

General SHWEDO. [The information is retained in the subcommittee files.]

QUESTIONS SUBMITTED BY MR. BROOKS

Mr. BROOKS. In 2017, Congress realized that there was a pressing need for someone to take the reigns and develop a capability that would allow for real time active cyber defense methods to be operationally fielded to protect small and medium sized businesses and organizations within the critical defense and industry infrastructure arena. SAC–D appropriated, and Congress funded, both in FY18 and FY19, the creation of a Cyber Security Operations Center (CSOC) to utilize DOD capabilities and experience to provide this capability to industry as an active defense measure, incor-

porating and leveraging off of a number of previously funded government and private initiatives. In light of the recently published National Cyber Strategy, and more pointedly the recently signed joint DOD/DHS MOA mandating the cooperation of these two Agencies in the cyber domain, what are the current plans for DHS to jointly utilize the Congressionally funded DOD CSOC being developed under the oversight of the Threat Systems Management Office (TSMO) within the PEO STRI to provide active defense cyber security measures to industries and organizations within the DOD/DHS realm of critical infrastructure?

Ms. MANFRA. [The information was not available at the time of printing.]

Mr. BROOKS. In 2017, Congress realized that there was a pressing need for someone to take the reigns and develop a capability that would allow for real time active cyber defense methods to be operationally fielded to protect small and medium sized businesses and organizations within the critical defense and industry infrastructure arena. SAC–D appropriated, and Congress funded, both in FY18 and FY19, the creation of a Cyber Security Operations Center (CSOC) to utilize DOD capabilities and experience to provide this capability to industry as an active defense measure, incorporating and leveraging off of a number of previously funded government and private initiatives. In light of the recently published National Cyber Strategy, and more pointedly the recently signed joint DOD/DHS MOA mandating the cooperation of these two Agencies in the cyber domain, what are the current plans for DHS to jointly utilize the Congressionally funded DOD CSOC being developed under the oversight of the Threat Systems Management Office (TSMO) within the PEO STRI to provide active defense cyber security measures to industries and organizations within the DOD/DHS realm of critical infrastructure?

Secretary RAPUANO. [The information is retained in the subcommittee files.]

Mr. BROOKS. In 2017, Congress realized that there was a pressing need for someone to take the reigns and develop a capability that would allow for real time active cyber defense methods to be operationally fielded to protect small and medium sized businesses and organizations within the critical defense and industry infrastructure arena. SAC–D appropriated, and Congress funded, both in FY18 and FY19, the creation of a Cyber Security Operations Center (CSOC) to utilize DOD capabilities and experience to provide this capability to industry as an active defense measure, incorporating and leveraging off of a number of previously funded government and private initiatives. In light of the recently published National Cyber Strategy, and more pointedly the recently signed joint DOD/DHS MOA mandating the cooperation of these two Agencies in the cyber domain, what are the current plans for DHS to jointly utilize the Congressionally funded DOD CSOC being developed under the oversight of the Threat Systems Management Office (TSMO) within the PEO STRI to provide active defense cyber security measures to industries and organizations within the DOD/DHS realm of critical infrastructure?

General SHWEDO. [The information is retained in the subcommittee files.]

QUESTIONS SUBMITTED BY MR. SUOZZI

Mr. SUOZZI. Please describe the current process for sharing cyber threat intelligence information between DOD and DHS, including classified indications and warnings. How is this done with other U.S. departments and agencies?

In your open testimony, you stressed the importance of receiving threat intelligence back from these partners. What is the process for receiving that information?

Ms. MANFRA. [The information was not available at the time of printing.]

Mr. SUOZZI. Please describe the current process for sharing cyber threat intelligence information between DOD and DHS, including classified indications and warnings. How is this done with other U.S. departments and agencies?

In your open testimony, you stressed the importance of receiving threat intelligence back from these partners. What is the process for receiving that information?

Secretary RAPUANO. In accordance with the Cybersecurity Information Sharing Act of 2015 and Presidential Policy Directive 41, United States Cyber Incident Coordination, DOD actively characterizes and assesses foreign cybersecurity threats and informs DHS of current and potential malicious cyberspace activity. DOD intelligence components, such as the National Security Agency (NSA), may provide technical assistance to U.S. Government departments and agencies when requested. In addition, the Secretary of Defense may approve providing DOD support to civil authorities in accordance with applicable law and policy. Specifically, three DOD centers are part of the established Federal Cybersecurity Centers designed to enhance information sharing, maintain situational awareness of cyber threats and incidents, and serve as conduits to DHS through its National Cybersecurity and Communications Integration Center (NCCIC) and Office of Intelligence and Analysis. These cen-

ters include NSA's Cybersecurity Threat Operations Center (NCTOC), the DOD Cyber Crime Center (DC3), and U.S. Cyber Command's (USCYBERCOM's) Joint Operations Center (JOC).

- The NCTOC is the 24/7/365 NSA element that characterizes and assesses foreign cybersecurity threats, and informs partners, such as DHS, of current and potential malicious cyberspace activity through its analysis of foreign intelligence with a focus on adversary computer network attacks, capabilities, and exploitations.
- DC3 supports DOD's law enforcement, counterintelligence, information assurance, network defense, and critical infrastructure protection communities through digital forensics, focused threat analysis, and training. The Secretary of Defense may elect to use DC3 to provide analytical and technical capabilities to DHS mission partners conducting national cyber incident response.
- The USCYBERCOM JOC directs the U.S. military's cyber operations and defense of the Department of Defense Information Network (DODIN). USCYBERCOM manages both the threat and asset response for the DODIN during incidents affecting the DODIN and shares cyber threat intelligence information as needed.

DOD shares cyber threat intelligence information with other Federal departments and agencies using a similar process in close collaboration with the Intelligence Community and the remaining Federal Cybersecurity Centers. Operated by the Office of the Director of National Intelligence, the Cyber Threat Intelligence Integration Center (CTIIC) is central to intelligence integration, analysis, and supporting activities for the Federal Government. The CTIIC has DOD participation, including by the Defense Intelligence Agency and NSA, and provides integrated all-source analysis of intelligence related to foreign cyber threats or related cyber incidents affecting U.S. national interests. CTIIC coordinates development of Federal intelligence information for the other Federal cybersecurity centers and Federal stakeholders. In coordination with the Defense Intelligence Enterprise, this could include pursuing declassification of intelligence and/or "tear-line" reports at different classification levels, as appropriate to the circumstances of the incident and to overall U.S. equities. DOD is also a member of the Cyber Unified Coordination Group that leverages DOD centers for their enhanced coordination procedures, above steady-state capacity, and/or operational or support personnel used to share cyber threat intelligence information.

The requirement to share intelligence and information is bi-directional, and it is not confined to DOD and DHS. Although the National Cyber Incident Response Plan outlines the when, what, and how to report cyber incidents to the Federal Government, most industry and private sector entities are reluctant to share related cyber threat information or submit a request for technical assistance. Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to DHS's NCCIC, the local field offices or national centers of Federal law enforcement agencies, or their sector specific agency. DOD is prepared to work with other Federal departments and agencies, when authorized to do so, to help affected entities understand the incident, link related incidents, and share information to resolve the situation rapidly and in a manner that protects privacy and civil liberties.

Mr. SUOZZI. Please describe the current process for sharing cyber threat intelligence information between DOD and DHS, including classified indications and warnings. How is this done with other U.S. departments and agencies?

In your open testimony, you stressed the importance of receiving threat intelligence back from these partners. What is the process for receiving that information?

General SHWEDO. [The information is retained in the subcommittee files.].

○