AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–597

THE ROLES AND RESPONSIBILITIES FOR DEFENDING THE NATION FROM CYBER ATTACK

HEARING

BEFORE THE

COMMITTEE ON ARMED SERVICES UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

OCTOBER 19, 2017

Printed for the use of the Committee on Armed Services

Available via the World Wide Web: http://www.govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
36–192 PDF WASHINGTON : 2019

COMMITTEE ON ARMED SERVICES

JOHN MCCAIN, Arizona, *Chairman*

JAMES M. INHOFE, Oklahoma	JACK REED, Rhode Island
ROGER F. WICKER, Mississippi	BILL NELSON, Florida
DEB FISCHER, Nebraska	CLAIRE MCCASKILL, Missouri
TOM COTTON, Arkansas	JEANNE SHAHEEN, New Hampshire
MIKE ROUNDS, South Dakota	KIRSTEN E. GILLIBRAND, New York
JONI ERNST, Iowa	RICHARD BLUMENTHAL, Connecticut
THOM TILLIS, North Carolina	JOE DONNELLY, Indiana
DAN SULLIVAN, Alaska	MAZIE K. HIRONO, Hawaii
DAVID PERDUE, Georgia	TIM KAINE, Virginia
TED CRUZ, Texas	ANGUS S. KING, JR., Maine
LINDSEY GRAHAM, South Carolina	MARTIN HEINRICH, New Mexico
BEN SASSE, Nebraska	ELIZABETH WARREN, Massachusetts
LUTHER STRANGE, Alabama	GARY C. PETERS, Michigan

CHRISTIAN D. BROSE, *Staff Director*
ELIZABETH L. KING, *Minority Staff Director*

CONTENTS

OCTOBER 19, 2017

	Page
THE ROLES AND RESPONSIBILITIES FOR DEFENDING THE NATION FROM CYBER ATTACK	1
Rapuano, Honorable Kenneth P., Assistant Secretary of Defense for Homeland Defense and Global Security, Department of Defense	4
Smith, Scott, Assistant Director for the Cyber Division, Federal Bureau of Investigation	10
Krebs, Christopher C., Performing the Duties of the Under Secretary for the National Protection and Programs Directorate, Department of Homeland Security	14
Questions for the Record	78

THE ROLES AND RESPONSIBILITIES FOR DEFENDING THE NATION FROM CYBER ATTACK

THURSDAY, OCTOBER 19, 2017

U.S. SENATE,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The committee met, pursuant to notice, at 9:36 a.m. in Room SD–G50, 13800 Senate Office Building, Senator John McCain, (chairman) presiding.

Committee members present: Senators McCain, Inhofe, Wicker, Fischer, Rounds, Ernst, Tillis, Sullivan, Sasse, Reed, Nelson, McCaskill, Shaheen, Gillibrand, Blumenthal, Donnelly, Hirono, Kaine, King, Heinrich, Warren, and Peters.

OPENING STATEMENT OF SENATOR JOHN MCCAIN, CHAIRMAN

Chairman MCCAIN. The committee meets today to receive testimony on the U.S. Government's policy, strategy, and organization to protect our Nation in cyberspace.

To begin, I would like to thank Senators Rounds and Nelson for their leadership on these issues in our Cybersecurity Subcommittee. This hearing builds upon the good work that they and their subcommittee have done this year to tackle the critical challenge of cyber.

This is a challenge that is growing more dire and more complex. Not a week passes that we do not read about some disturbing new incident: cyber attacks against our government systems and critical infrastructure, data breaches that compromise sensitive information of our citizens and companies, attempts to manipulate public opinion through social media, and of course attacks against the fundamentals of our democratic system and process. Those are just the ones that we know about.

This is a totally new kind of threat, as we all know. Our adversaries, both state and non-state actors, view the entire information domain as a battlespace, and across it, they are waging a new kind of war against us, a war involving but extending beyond our military, to include our infrastructure, our businesses, and our people.

The Department of Defense has a critical role to play in this new kind of war, but it cannot succeed alone. To be clear, we are not succeeding. For years, we have lacked policies and strategies to counter our adversaries in the cyber domain, and we still do. This is in part because we are trying to defeat a 21st Century threat with the organizations and processes of the last century. This is

true in the executive branch and, frankly, it is also true here in the Congress. We are failing.

That is why this committee is holding today's hearing and why we have taken the unorthodox step of inviting witnesses from across our government to appear today. Our witnesses are the senior officials responsible for cyber within their respective agencies, and I want to thank them for joining us and welcome them now: Ken Rapuano, Assistant Secretary of Defense for Homeland Defense and Global Security; Scott Smith, Assistant Director for Cyber Division, Federal Bureau of Investigation; and Chris Krebs, Under Secretary for the National Protection and Programs Directorate at the Department of Homeland Security.

I would also like to note at the outset the empty chair at the witness table. The committee invited the principal U.S. cyber official, White House Cybersecurity Coordinator Rob Joyce. Many of us know Mr. Joyce and respect him deeply for his significant experience and expertise on cyber and his many years of government service at the National Security Agency. Unfortunately, but not surprisingly, the White House declined to have its cyber coordinator testify, citing executive privilege and precedent against having non-confirmed NSC [National Security Council] staff testifying before Congress. While this is consistent with past practice on a bipartisan basis, I believe the issue of cyber requires us to completely rethink our old ways of doing business.

To me, the empty chair before us represents a fundamental misalignment between authority and accountability in our government today when it comes to cyber. All of our witnesses answer to the Congress for their part of the cyber mission. But none of them is accountable for addressing cyber in its entirety. In theory, that is the White House Cyber Coordinator's job, but that non-confirmable position lacks the full authority to make cyber policy and strategy and direct our Government's efforts. That official is literally prohibited by legal precedent from appearing before the Congress. So when we, the elected representatives of the American people, ask who has sufficient authority to protect and defend our Nation from cyber threats and who is accountable to us for accomplishing that mission, the answer is quite literally no one.

The previous administration's struggle to address this challenge between DOD [Department of Defense], DHS [Department of Homeland Security], and the FBI [Federal Bureau of Investigation], well-intentioned though it was, led to a result that is as complex and convoluted as it appears in this chart. Given that no single agency has all of the authorities required to detect, prevent, and respond to incidents, the model has created significant confusion about who is actually accountable for defending the United States from cyber attacks. Meanwhile, our increasingly capable adversaries continue to seek to exploit our vulnerabilities in cyberspace.

Facing similar challenges, a number of our allies have pursued innovative models to emphasize increased coordination and consolidation. In doing so, they have significantly enhanced their ability to react and respond to incidents and to share information across government and with the public. For example, the United Kingdom recently established its National Cyber Security Centre, an organi-

zation that orchestrates numerous cyber functions across the British Government under one roof sitting side by side with industry.

Today's hearing is an opportunity to have an honest and open conversation. Our concerns are not meant to be critical of our witnesses' leadership or of your organizations, as each of you are limited by the policy and legal frameworks established by Congress and the administration. Our intent is to better understand the coordination and de-confliction underway between agencies and to identify where and how we can improve. The last thing any of us wants is to waste precious time during a major cyber incident because everyone who rushed to the scene thought they were in charge, but none had the authority or, even worse, realizing after a cyber incident, that your organizations were not prepared and resourced to respond based on a flawed assumption that someone else was responsible.

I thank the witnesses for their service to our country and their willingness to appear before this committee as we continue to assess and address our cyber challenges.

Senator Reed?

STATEMENT OF SENATOR JACK REED

Senator REED. Well, thank you very much, Mr. Chairman, for holding this hearing.

I welcome our witnesses today.

Let me also commend Senator Rounds and Senator Nelson for their great leadership on the subcommittee.

The cyber threat facing our Nation does not respect organizational or jurisdictional boundaries in the Government. The Defense Department, the intelligence community, the FBI, the Department of Homeland Security are all critical in countering the cyber threat. But each agency functions in siloes under specialized laws and authorities. In order to be successful, we must develop an integrated, whole-of-government approach to strategic planning, resource allocation, and execution of operations. I think I am echoing the chairman's points.

This problem is not unique to the cybersecurity mission. Violent extremism, narcotics, and human trafficking, transnational crime, proliferation of weapons of mass destruction, and other challenges require an effective whole-of-government response that cut across the missions and responsibilities of departments and agencies. As issues become more complex, these cross-cutting problems are becoming more numerous and serious over time.

There have been various approaches to this problem, but with little demonstrated success. White House's czars generally have few tools at their disposal, while a lead agency designated to address a cross-cutting challenge must also remain focused on the mission of its own organization.

Last year, President Obama signed PPD [Presidential Policy Directive 41] 41, the United States Cyber Incident Coordination Policy. It established a cyber response group to pull together a whole-of-government response in the event of major cyber incidents. But these are ad hoc organizations with little continuity that come together only in response to events.

I believe what is needed instead is a framework with an integrated organizational structure authorized to plan and cooperate in peacetime against the constant aggression of cyber opponents. This arrangement has precedent. The Coast Guard is a service branch in the Department of Defense, but it is also a vital part of the Department of Homeland Security. It has intelligence authorities, defense responsibilities, customs and border enforcement, and law enforcement authority. The Coast Guard exercises these blended authorities judiciously and responsibly and enjoys the confidence of the American people. Therefore, we can solve this problem. We have examples of where we have solved this problem.

Last year's National Defense Authorization Act created cross-functional teams to address problems that cut across the functional organizations of the Defense Department. These teams are composed of experts from the functional organizations but rise above the parochial interests of their bureaucracies. The team leads would exercise executive authority delegated by the Secretary of Defense. Such an approach might be a model for the interagency to address a cross-cutting problem like cybersecurity.

There, indeed, is urgency to our task. Russia attacked our election last year. They similarly attacked multiple European countries, the NATO [North Atlantic Treaty Organization] alliance, and the European Union. The intelligence community assures us that Russia will attack our upcoming midterm elections. So far, we have seen no indication that the administration is taking action to prepare for this next inevitability.

Finally, the Government cannot do this alone. As former Cyber Commander and NSA [National Security Administration] Director General Keith Alexander testified, "While the primary responsibility of government is to defend the Nation, the private sector also shares responsibility in creating the partnerships necessary to make the defense of our nation possible. Neither the Government nor the private sector can capably protect their systems and networks without extensive and close cooperation." In many ways, the private sector is on the front lines of the cyber threat, and the Government must work with them if we are to effectively counter that threat. We need a government strategy, but it must be in cooperation with the private sector.

I thank Chairman McCain for holding this hearing and for cosponsoring my legislation that is in the Banking Committee's jurisdiction, S. 536, the Cybersecurity Disclosure Act, which through disclosure and our federal securities laws tries to encourage companies to focus on avoiding cybersecurity risks before they turn into costly breaches.

Thank you, Mr. Chairman.

Chairman MCCAIN. Welcome to the witnesses. Mr. Rapuano, please proceed.

STATEMENT OF HONORABLE KENNETH P. RAPUANO, ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY, DEPARTMENT OF DEFENSE

Mr. RAPUANO. Thank you, Chairman McCain, Ranking Member Reed, and members of the committee. It is an honor to appear before you to discuss the roles and responsibilities of the Department

of Defense and its interagency partners in defending the Nation from cyber attacks of significant consequence.

I am here today in my roles as the Assistant Secretary of Defense for Homeland Defense and Global Security, as well as the Principal Cyber Advisor to the Secretary of Defense, in which I oversee cyber policy in the Department, lead the coordination of cyber efforts across the Department and with our interagency partners, and integrate the Department's cyber capabilities with its mission assurance and defense support to civil authorities activities. I appreciate the opportunity to testify alongside my interagency colleagues because these challenges do require a whole-of-government approach.

DOD is developing cyber forces and capabilities to accomplish several missions in cyberspace. Today, I will focus on our mission to defend the United States and its interests against high consequence cyber attacks and how we execute that mission in coordination with our interagency partners.

The Department's efforts to build defensive capabilities through the Cyber Mission Force, or CMF, play an especially key role in carrying out this mission. From both a deterrence and response standpoint, the 133 CMF teams that will attain full operational capability in September of 2018 are central to the Department's approach to supporting U.S. Government efforts to defend the Nation against significant cyber attacks. With the goal of assuring U.S. military dominance in cyberspace, these teams conduct operations both to deny potential adversaries the ability to achieve their objectives and to conduct military actions in and through cyberspace to impose costs in response to an imminent, ongoing, or recent attack.

In particular, the CMF's 68 Cyber Protection Teams represent a significant capability to support a broader domestic response. These forces are focused on defending DOD information networks, but select teams could provide additional capacity or capability to our federal partners, if and when necessary.

DOD's role in cyberspace goes beyond adversary-focused operations and includes identifying and mitigating our own vulnerabilities. Consistent with statutory provisions related to these efforts, we are working with our U.S. domestic partners and with foreign partners and allies to identify and mitigate cyber vulnerabilities in our networks, computers, critical DOD infrastructure and weapons systems.

While DOD has made significant progress, there is more to do alongside with our other agency partners in the broader whole-of-government effort to protect U.S. national interests in and through cyberspace. The outward focus of DOD's cyber capabilities to mitigate foreign threats at their points of origin complements the strengths of our interagency partners as we strive to improve resilience, should a significant cyber attack occur. In accordance with law and policy, during cyber incidents, DOD can be called to directly support the DHS in its role as the lead for protecting, mitigating, and recovering from domestic cyber incidents or the DOJ in its role as the lead in investigating, attributing, disrupting, and prosecuting cyber crimes.

The significant work of our Departments has resulted in increased common understanding of our respective roles and respon-

sibilities, as well as our authorities. Despite this, however, as a government we continue to face challenges when it comes to cyber incident response on a large scale, and it is clear we have more work to ensure we are ready for a significant cyber incident. Specifically, we must resolve seam and gap issues among various departments, clarify thresholds for DOD assistance, and identify how to best partner with the private sector to ensure a whole-of-nation response, if and when needed.

DOD has a number of efforts underway to address these challenges and to improve both our readiness and that of our interagency partners. For instance, we are refining policies and authorities to improve the speed and flexibility to provide support, and we are conducting exercises such as Cyber Guard with a range of interagency and State and local partners to improve our planning and preparations to respond to cyber attacks.

Additionally, the cyber executive order 13800 signed in May will go a long way in identifying and addressing the shortfalls in our current structure.

Although the Department has several unique and robust capabilities, I would caution against ending the current framework and reassigning more responsibility for incident response to DOD. The reasons for this include the need for the Department to maintain focus on its key mission, the longstanding tradition of not using the military for civilian functions, and the importance of maintaining consistency with our other domestic response frameworks.

It is also important to recognize that a significant realignment of cyber response roles and responsibilities risks diluting DOD focus on its core military mission to fight and win wars.

Finally, putting DOD in a lead role for domestic cyber incidents would be a departure from accepted response practice in all other domains in which civilian agencies have the lead responsibility for domestic emergency response efforts. It could be disruptive to establishing that critical unity of effort that is necessary for success.

The Federal Government should maintain the same basic structure for responding to all other national emergencies, whether they are natural disasters or cyber attacks.

There is still work to be done both within the Department and with our federal partners to improve DOD and U.S. Government efforts overall in cyberspace. Towards this end, I am in the process of reinvigorating the role of the Principal Cyber Advisor, clarifying the Department's internal lines of accountability and authority in cyber, and better integrating and communicating DOD cyberspace strategy, plans, and train and equip functions. We will also be updating our DOD cyber strategy and policies on key cyber issues, such as deterrence, and translating this guidance into capabilities, forces, and operations that will maintain our superiority in this domain.

The Department is also working to ensure that several strategic initiatives it is undertaking come to fruition, including the elevation of U.S. Cyber Command, the implementation of the cyber executive order, initiating the cyber excepted service program, and rationalizing the Department's cyber budget and investments.

Our relationship with Congress is critical to everything we are doing to defend the Nation from high consequence cyber attacks. I

am grateful for Congress' strong support and particularly this committee's interest in these issues. I look forward to your questions and working with you and your staff's going forward. Thank you.

[The prepared statement of Mr. Rapuano follows:]

PREPARED STATEMENT BY MR. KENNETH RAPUANO

Thank you Chairman McCain, Ranking Member Reed, and Members of the Committee. It is an honor to appear before you to discuss the roles and responsibilities for defending the Nation from cyberattacks of significant consequence. I appear before you today in my role as Assistant Secretary of Defense for Homeland Defense and Global Security and as Principal Cyber Advisor to the Secretary of Defense. In these roles, I oversee the development and implementation of DOD's strategy, policy, and strategic guidance to achieve DOD's cyber missions, goals, and objectives; lead the Department's interagency cyber coordination efforts, including for cyber incident response; advise the Secretary and the Deputy Secretary on cyber-related activities that support or enable DOD's missions in and through cyberspace; and, perhaps most relevant to today's discussion, ensuring that cyber forces and capabilities are integrated across all of DOD's priority missions, including mission assurance and Defense Support of Civil Authorities.

I have been requested to discuss the Department's role as part of an interagency response to a cyberattack of significant consequence. I am grateful to testify alongside my interagency colleagues because adequately addressing these important challenges requires a whole-of-government approach, of which the Department of Defense and its developing capabilities in cyberspace are just one part.

This is a timely and important topic because the threats and level of malicious activity we face in cyberspace are real and growing. This diverse and persistent set of threats comes from state and non-state actors who probe and scan United States. networks for vulnerabilities. The states we watch most closely in cyberspace include China, Iran, North Korea, and especially Russia.

To address these threats, the Department is developing cyber forces and capabilities to accomplish three primary missions in cyberspace: 1) to defend DOD networks, systems, and information to ensure that DOD can accomplish its core missions; 2) to defend the United States and its interests against malicious cyber activities and cyberattacks of significant consequence; and 3) to provide integrated cyber capabilities in support of operational and contingency plans. Although all of the missions are important, given your focus today, my intent is to speak primarily about DOD's efforts to defend the United States and its interests from cyberattacks of significant consequence and its efforts to provide Defense Support for Civil Authorities, as these define DOD's role within a whole-of-government framework.

The Cyber Mission Force (CMF) is the Department's principal capability to carry out DOD's cyber mission. Consisting of more than 6,000 soldiers, sailors, airmen, marines, and civilians, the CMF achieved initial operational capability (IOC) in October 2016 and is projected to reach full operational capacity (FOC) by the end of this new fiscal year. Today, nearly 80 percent of the CMF's 133 teams have reached FOC. In recent years, the Department has made significant investments in building the workforce and systems to develop the CMF, and it continues to do so consistent with the fiscal year 2018 budget request. In terms of readiness, as well as operational activities in support of the campaign to defeat the Islamic State in Iraq and Syria (ISIS), DOD is already seeing the results of those investments. United States Cyber Command's increased experience, expertise, and capability drove the President's decision this summer to elevate U.S. Cyber Command to a Unified Functional Combatant Command, consistent with section 923 of the National Defense Authorization Act of for fiscal year 2017. Among other benefits, elevation of the command will strengthen command and control and consolidate responsibility for cyberspace operations under a single commander, reporting directly to the Secretary.

Although many elements of the CMF contribute to defending the Nation against malicious cyber activities and cyberattacks of significant consequence, the Cyber National Mission Force through its integrated operations plays a key role. This force combines the capabilities of National Mission Teams (NMTs) that pursue adversaries into red space; National Support Teams (NSTs) that provide additional capacity in analysis, linguists, reporting, capability development, and targeting; and national Cyber Protection Teams (CPTs) that hunt adversaries in friendly terrain. As the primary counter-cyber forces, the integration of NMTs, NSTs, and national CPTs enhances our ability to learn the tactics, techniques, and procedures of our adversaries to detect malicious cyber activity. These teams develop and, if directed, undertake operations to deter, delay, disrupt, and defeat an imminent or ongoing

cyberattack or malicious cyber activity. The combined efforts of these teams give the CMF the capacity to operate on a global scale against the broad spectrum of adversaries and growing threats.

Additionally, DOD is developing significant cyber capability and capacity within the Reserve Components, including the National Guard. The Air National Guard is developing 12 Air National Guard Squadrons to provide two full-time CPTs through rotations and is also providing three additional squadrons to deliver a portion of an NMT to the CMF. The Army National Guard has established the first of 11 CPTs, which will be built out through 2022. The U.S. Army Reserve will follow by establishing 10 teams of its own between now and 2024. Likewise, the Air Force Reserve is contributing personnel to fill three CPTs. All of these teams benefit from strong relationships with State and local authorities. To further strengthen these relationships and support preparedness, National Guard units may coordinate with, train, advise, and assist governmental entities outside DOD when incidental to military training in accordance with section 2012 of title 10, U.S. Code.

From both a deterrence and response standpoint, CMF teams are central to the Department's approach to cyber operations and to support U.S. Government efforts to defend the Nation against a cyber incident of significant consequence. With a goal of ensuring U.S. military dominance in cyberspace, these teams support the Department's efforts to deny the adversary the ability to achieve its objectives and, when directed, to conduct military actions in and through cyberspace in response to an imminent, ongoing, or recent attack or malicious cyber activity. Although DOD's focus is on preparing for and defending against cyberattacks of significant consequence, the President may determine that a military response to malicious cyber activity below the threshold of significant consequence or an armed attack is necessary and appropriate.

DOD's role in cyberspace goes beyond adversary-focused operations and includes identifying and mitigating our own vulnerabilities. DOD recognizes its own reliance on cyber-enabled critical infrastructure to conduct its core missions. The Department therefore understands congressional concerns regarding current and future cyber vulnerabilities and congressional efforts to authorize vulnerability identification programs. In response, we are working with our foreign partners and allies and our U.S. domestic partners, including the Department of Homeland Security (DHS), to identify cyber vulnerabilities in our networks, computers, critical DOD infrastructure, and weapon systems. In addition to these external partnerships, the Department is leveraging its own mission assurance risk-management processes to identify, prioritize, and mitigate the most impactful vulnerabilities to the critical infrastructure that is fundamental to DOD's ability to project power and protect the U.S. Homeland, our people, and our allies and partners.

One last important element of our mission to defend the Nation is the Department's role as the sector-specific agency for the Defense Industrial Base (DIB), one of the 16 identified critical infrastructure sectors. Using voluntary and mandatory reporting requirements, the Department partners with DIB sector stakeholders to maintain a robust cybersecurity and information assurance program to protect sensitive defense information and protect DOD networks and systems.

DOD has made significant progress; however, there is more to do, and we are only one piece of the broader whole-of-government effort to protect U.S. national interests in and through cyberspace. The outward, threat focus of DOD's cyber capabilities complements the strengths of our interagency partners, as we strive to improve resilience should a cyberattack of significant consequence occur. As articulated in law and policy, during cyber incidents, DOD may directly support the DHS's lead for protecting, mitigating, and recovering from domestic cyber incidents or, as appropriate and authorized by law, the Department of Justice's (DOJ) lead in investigating, attributing, disrupting, and prosecuting cybercrimes. Under DOD's broader Defense Support of Civil Authorities mission, the Department works closely with these domestic partners as they carry out their aforementioned responsibilities so that DOD is prepared to provide support when it is needed and DOD is called upon to do so. DOD also regularly works closely with domestic partners through cyber fusion center integration, robust information sharing arrangements, liaison and detailee programs, development of national plans, exercises to strengthen our response, and interagency deliberations on malicious cyber activity.

The significant work of U.S. departments and agencies has resulted in a common understanding of our various roles, responsibilities, and authorities. That said, it is clear we have more work to do to resolve seam and gap issues among various departments and agencies. DOD has taken a number of steps to address these problems and to improve both our readiness and that of our interagency partners. For instance, we are continually refining policies and authorities to improve the speed and flexibility to provide support, and we organize and participate in exercises, such

as CYBER GUARD, with a range of interagency, State, and local partners to improve our ability to respond to cyberattacks on critical infrastructure.

Although DOD has built capacity and unique capabilities, for a number of reasons, I would caution against ending the current framework and against reassigning more responsibility for incident response to the Department of Defense. First, DOD's primary mission is to provide the military forces needed to deter war and to be prepared to defend the country should deterrence fail, which requires us to be prepared at all times to do so. DOD is the only department or agency charged with this mission, and success in this requires the Department's complete focus. In this case, any significant realignment of roles and responsibilities will have opportunity costs, including absorptive capacity to build mission capability in a new area, especially ones that could distract the Department from its core warfighting missions.

Second, the United States has a long normative and legal tradition limiting the role of the military in domestic affairs. This strict separation of the civilian and the military is one of the hallmarks of our democracy and was established to protect its institutions. Designating DOD as the lead for the domestic cyber mission risks upsetting this traditional civil-military balance.

Third, a primary civil reliance on DOD in the steady-state would result in increased demands that could not be met without significant changes in resource allocation. We would expect even greater demand in a conflict scenario, when there might be a natural tension in the need to preserve DOD mission capabilities and requests for support to civilian agencies. Even with such a change in resource allocation, the addition of a new mission would likely detract from the focus on and readiness for the warfighting mission.

Finally, putting DOD in a lead role for cyber incidents creates an exception to accepted domestic response practice in all other domains, which would disrupt our efforts to establish and maintain unity of effort. Civilian agencies have the lead responsibility for domestic emergency response efforts; this should not be different for cyber incidents. The Federal Government should maintain a common approach to all national emergencies, whether they are natural disasters or cyberattacks.

I have confidence that the President's Executive Order 13800 signed in May will address many of Congress's concerns by helping to identify and address the shortfalls in the present system. Through reports and other deliverables, the Executive Order specifically targets the areas of protecting critical infrastructure, strengthening the deterrence posture of the United States, and building international coalitions. As a result, the Federal Government—especially DHS and Sector Specific Agencies—is identifying current and prospective authorities and capabilities that it could use to support the cybersecurity efforts of critical infrastructure entities. DOD is contributing to these efforts and conducting its own review of how best to protect the Defense Industrial Base from cyber vulnerabilities. Through this process, we should have a better understanding of the key challenges facing the U.S. Government in this area and a way forward for addressing them.

Therefore, my vision and highest priority in cyber are to address the challenges that still face the Department in cyberspace and its role in the broader interagency response effort. Specifically, I am working to reinvigorate the role of the Principal Cyber Advisor; to clarify the Department's internal lines of accountability and authority in cyber; and to integrate and communicate more effectively DOD cyberspace strategy, plans, and train and equip functions in cyber. It is also time to revise our Cyber Strategy, update policy on such key cyber issued as deterrence, and translate this and other guidance into capabilities, forces, and operations that will maintain our superiority in this domain. Meanwhile, the Department must ensure that several strategic initiatives it is undertaking in cyber come to fruition, including the elevation of U.S. Cyber Command to a unified combatant command, implementing the Cyber Executive Order, initiating the Cyber Excepted Service, and identifying and mitigating vulnerabilities in DOD's networks, systems, and platforms. I look forward to working with Congress on these efforts and welcome its feedback.

In conclusion, the Department of Defense is committed to defending the U.S. Homeland and is prepared to defend the Nation from cyberattacks of significant consequence that may occur in or through cyberspace. It has undertaken comprehensive efforts, both unilaterally and in concert with interagency partners, allies, and the private sector to improve our Nation's cybersecurity posture and to ensure that DOD has the ability to operate in any environment at any time. Our relationship with Congress is absolutely critical to everything the Department is doing. To that end, I am grateful for Congress's strong support and particularly this Subcommittee's interest in these issues, and I look forward to your questions.

Chairman MCCAIN. Thank you.

Mr. Smith?

STATEMENT OF SCOTT SMITH, ASSISTANT DIRECTOR FOR THE CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. SMITH. Thank you, Mr. Chairman, and thanks to the committee for offering me an opportunity to provide remarks on the FBI's cyber capabilities.

As the committee is aware, the frequency and sophistication of cyber attacks on our Nation have increased dramatically in the past decade and only look to be growing. There are significant challenges. The cyber domain is unique, constantly shifting, changing, and evolving. But progress has been made in improving structures and collaboration in innovation. But more can be done.

Staying ahead of today's threats requires a different mindset than in the past. The scale, scope, and complexity of today's threats in the digital domain is unlike anything humanity or our Nation has ever experienced. Traditional approaches and mindsets are no longer suited to coping with the speed and mobility and complexity of the new digital domain. We have to include the digital domain as part of the threat ecosystem instead of separating it as a mechanical machine. This new era, often called the Fourth Industrial Revolution, requires the FBI to rapidly assign, align, and engage empowered networked teams who are purpose-driven and have fierce and unrelenting resolve to win.

What does this all mean? What are we doing to meet and stay ahead of the new digital domain, attribute, predict, impose consequences?

That is where the FBI cyber mission is going. The FBI Cyber Division and program is structured to address a lot of these unique set of challenges.

In the field, the FBI is made up of 56 different field offices spanning all 50 States and U.S. territories, each with a cyber squad and each developing multi-agency cyber task forces which brings together technically proficient investigators, analysts, computer scientists from local, State, and Federal organizations.

At FBI headquarters, in addition to those field resources, the Cyber Division offers program management and coordination and more technically advanced responders in our Cyber Action Teams. The CAT [Cyber Action Team] teams, our elite cyber rapid response force, is on call and prepared to deploy globally in response to significant cyber incidents.

Additionally at FBI headquarters, we manage CyWatch, a 24-hour watch center which provides continuous connectivity to interagency partners in an effort to facilitate information sharing and real-time incident management and tracking, ensuring all agencies are coordinating.

In addition to these cyber-specific resources, the FBI has other technical assets that can be utilized in the event of cyber incidents. These include our Operational Technology Division, the Regional Computer Forensic Laboratory Program, and the Critical Incident Response Group providing additional expertise and capabilities and resources that the FBI can leverage at a cyber incident.

Partnerships are absolutely a key focus area for the FBI. We rely on a robust international presence to supplement our domestic footprint. Through cyber assistant legal attaches, the FBI embeds cyber agents with our international counterparts in 18 key loca-

tions across the globe. The FBI also relies upon private sector partnerships leveraging the National Cyber Forensic Training Alliance, InfraGard, and Domestic Security Alliance, just to name a few.

Building capacity at home and abroad through training, investigations, and joint operations is where we are applying our efforts.

The FBI has the capability to quickly respond to cyber incidents across the country and scale its response to the specific incident utilizing all its resources throughout the field, headquarters, and abroad. We have the ability to galvanize and direct all the available cyber resources instantaneously.

Utilizing dual authorities as a domestic law enforcement organization and a member of the U.S. intelligence community, the FBI works closely with interagency partners within a whole-of-government effort to countering cyber threats.

The FBI conducts its cyber mission with the goal of imposing costs and consequence on the adversary. Though we would like to arrest every cyber criminal, we recognize indictments are just one tool in a suite of options that are available to the U.S. Government when deciding how best to approach this complex cyber threat.

The FBI understands the importance of being coherently joined with, and we will continue to find ways to work with interagency partners in responding to cyber incidents. We look forward to expanding our partnerships with Cyber Command, given their new and unique capabilities, and with the National Guard's new cyber program in complementing our field offices and cyber task forces, all within the confines of current laws, authorities, and expectations of the American people.

We at the FBI appreciate this committee's efforts in making cyber threat a focus and committing to improving how we can work together to better defend our Nation. We also look forward to discussing these issues in greater detail and answering any questions that you may have.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT BY SCOTT S. SMITH

Chairman McCain, Ranking Member Reed, and members of the Committee, thank you for the invitation to provide remarks on the FBI's role in defending the Nation against cyber threats.

As the Committee is well aware, the frequency and impact of cyberattacks on our nation's private sector and government networks have increased dramatically in the past decade and are expected to continue to grow. We continue to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. Within the FBI, we are focused on the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers and global organized crime syndicates, as well as other technically sophisticated attacks.

Cyber threats are not only increasing in scope and scale, they are also becoming increasingly difficult to investigate. Cyber criminals often operate through online forums, selling illicit goods and services, including tools that can be used to facilitate cyber attacks. These criminals have also increased the sophistication of their schemes, which are more difficult to detect and more resilient. Additionally, many cyber actors are based abroad or obfuscate their identities by using foreign infrastructure, making coordination with international law enforcement partners essential.

The FBI has worked with the rest of the intelligence and law enforcement community to address the unique set of challenges presented by the cyber threat. The in-

formation domain is an inherently different battle space, requiring government bureaucracies to shift and transform to eliminate duplicative efforts and stovepipes and move toward real-time coordination and collaboration to keep pace with the growing threat. Considerable progress has been made toward the shared goal of protecting the country from capable and unrelenting cyber adversaries, but there is still a lot to be done to ensure our government agencies have the proper resources, structure, and mission to seamlessly work together on the cyber threat. The FBI will continue to be a leader in this area, and we have taken a number of steps in the last several years to ensure we are adequately structured to respond to threats in an agile and efficient way.

The decentralized FBI field structure is intended to support the investigation of crimes across the Nation. The FBI is made up of 56 field offices spanning all 50 States and U.S. territories, each with a multi-agency Cyber Task Force ("CTF") modeled after the successful Joint Terrorism Task Force program. The task forces bring together cyber investigators, prosecutors, intelligence analysts, computer scientists, and digital forensic technicians from various Federal, State, and local agencies present within the office's territory. Our field-centric business model allows us to develop relationships with local companies and organizations, putting us in an ideal position to engage with potential victims of cyber attacks and crimes. Cyber-trained special agents are in each field office, providing locally available expertise to deploy to victim sites immediately upon notice of an incident. Computer scientists and intelligence analysts are also stationed in field offices to support incident response efforts and provide intelligence collection and analysis as well as technical assistance and capability.

In addition to the resources in the field, the FBI has the Cyber Action Team ("CAT"), Cyber Division's elite rapid response force. On-call CAT members are prepared to deploy globally to bring their in-depth cyber intrusion expertise and specialized investigative skills to bear in response to significant cyber incidents. CAT's management and core team are based at headquarters, supplemented by carefully selected and highly trained field personnel. CAT members are available to supplement the technical capabilities in the field, and they are typically deployed in support of significant cyber incidents that have the potential to impact public health or safety, national security, economic security, or public confidence.

Cybersecurity threats and incidents are occurring around the clock, which motivated Cyber Division in 2014 to establish a steady-state 24-hour watch capability called CyWatch. Housed at the National Cyber Investigative Joint Task Force ("NCIJTF"), CyWatch is responsible for coordinating domestic law enforcement response to criminal and national security cyber intrusions, tracking victim notification, and coordinating with the other Federal cyber centers many times each day. CyWatch provides continuous connectivity to interagency partners to facilitate information sharing and real-time incident management and tracking as part of an effort to ensure all agencies are coordinating. CyWatch also manages FBI's Cyber Guardian program, through which more than 5,000 victim notifications were logged and coordinated in fiscal year 2016.

In addition to these cyber specific resources, the FBI has other technical assets that can be utilized as necessary to combat cyber threats. Our Operational Technology Division develops and maintains a wide range of sophisticated equipment, capabilities, and tools to support investigations and assist with technical operations. The FBI maintains a robust forensic capability through its Regional Computer Forensic Laboratory Program, a national network of FBI-sponsored digital forensics laboratories and training centers devoted to the examination of digital evidence. The Critical Incident Response Group ("CIRG") provides crisis support and incident management assistance. These resources can be leveraged throughout the FBI's response and investigative cycle to respond to cyber threats.

Given the international nature of cybercrime and the reality that the actors who seek to harm the U.S. through cyber means are often located abroad, the FBI relies on a robust international presence to supplement its domestic footprint. Through the Cyber Assistant Legal Attache ("Cyber ALAT") program, the FBI embeds cyber agents, who are trained both at FBI Headquarters and in the field, with our international counterparts in 18 key locations across the globe where they build relationships with our international partners. These relationships are essential to working cyber cases that often involve malicious actors using computer networks worldwide.

In order to be successful in the mission of bringing cyber criminals to justice and deterring future activity in the cyber realm, the FBI relies on partnerships with the private sector. As frequent targets of malicious cyber activity, the private sector is on the front lines of defending our nation's critical information infrastructure, safeguarding its intellectual property, and preserving its economic prosperity. By building and maintaining partnerships with industry, the FBI is better able to share in-

formation about current and future threats, provide indicators of compromise for network defense, and provide context to help companies understand the intent behind the unnamed actors targeting their systems. These relationships also provide an optic into what kinds of nefarious activity they are observing on their systems, which helps the FBI better understand the threats.

The FBI has the capability to quickly respond to cyber incidents across the country and scale its response to the specific circumstances of the incident by utilizing all resources at its disposal throughout the field, at FBI headquarters, and abroad. Utilizing dual authorities as a domestic law enforcement organization and a member of the U.S. Intelligence Community ("USIC"), the FBI works closely with interagency partners in a whole-of-government approach to countering cyber threats. Presidential Policy Directive 41, signed by President Obama in July 2016, designates the Department of Justice, through the FBI and NCIJTF, as the lead Federal agency for threat response. Threat response is defined as activities related to the investigation of an incident and the pursuit, disruption, and attribution of the threat actor. Through evidence collection, technical analysis, disruption efforts, and related investigative tools, the FBI works to quickly identify the source of a breach, connect it with related incidents, and determine attribution, while developing courses of action.

The FBI is able to collect domestic intelligence on cyber threats, consistent with our authorities, to help us understand and prioritize identified threats, reveal intelligence gaps, and fill those gaps. By combining this intelligence with information from our interagency partners, the FBI contributes to painting a collective picture of cyber threats facing the Nation. This threat intelligence is critical to getting ahead of the threat and providing potential victims with information to assist them in better protecting their networks from compromise. The FBI liaises with the other intelligence community components through standing coordination calls among the various watch centers; participation in standing interagency groups as well as incident- and threat-based working groups; through embeds and liaison officers at other agencies and within the FBI; and through memoranda of understanding allowing close coordination on topics of high importance.

The FBI along with the rest of the intelligence community understands the need to share information both within and outside the Government with the potential victims of cyber attacks. The FBI disseminates information regarding specific threats to the private sector through various methods, including Private Industry Notifications ("PINs") and FBI Liaison Alert System ("FLASH") reports. PINs provide unclassified information that will enhance the private sector's awareness of a threat, and FLASH reports contain unclassified technical information collected by the FBI for use by specific private sector partners. These communication methods facilitate the sharing of information with a broad audience or specific sector. The FBI also works with industry partners in forums such as InfraGard and industry-based Information Sharing and Analysis Centers ("ISACs") to relay critical information. The FBI also works closely with its government partners to put out joint notifications and reports to help the private sector guard against potential cyber threats.

In some cases, the FBI receives indicators of potential compromise from various sources, including USIC partners and foreign governments, that are used in notification to victims of cyber attacks. Victim notification is critical in preventing continued cyber intrusion activity and mitigating the damages associated with the theft of sensitive data, intellectual property, and proprietary information. The goal of notification is to provide timely and meaningful notification to the victim while protecting sensitive sources and methods and balancing investigative and operational equities of the FBI and other USIC agencies. FBI and the Department of Homeland Security (DHS) have well defined policies and procedures which guide how victims are identified and how notification should be made; typically, the FBI, in coordination with DHS, will notify the individuals responsible for handling network security for the victim organization to discuss the necessary information related to the intrusion. The FBI will also provide open source information that may assist in the detection and identification of the intrusion. After the initial notification, some victims will contact the FBI to provide an update regarding the compromise of their network, while others will not. Typically, any post-notification engagement between the FBI and the victim is voluntary and its scope is determined by the company.

The FBI conducts its cyber mission with the goal of imposing costs on the adversary, and though we would like to arrest every cyber criminal who commits an offense against a U.S. person, company, or organization, we recognize indictments are just one tool in a suite of options available to the U.S. Government when deciding how best to approach complex cyber threats. Working with the rest of the USIC, the FBI is able to share intelligence, better understand the threat picture, identify additional victims or potential victims of cyber intrusions, and help inform U.S. pol-

icymakers. The FBI and the intelligence community must work closely on cyber threats to provide leaders with the information necessary to decide what tools are appropriate to respond to, mitigate, and counter cyber attacks, as well as deter cyber actors and reinforce peacetime norms of state behavior in cyberspace.

Using unique resources, capabilities, and authorities, the FBI is able to impose costs on adversaries, deter illicit cyber activity, and help prevent future cyber attacks. While much progress has been made toward leveraging the FBI's unique authorities and resources in real-time coordination with the interagency to combat cyber threats, there is still work to be done, specifically in ensuring agile and efficient incident response, seamless information sharing, and elimination of duplicative efforts. Although the resources of the FBI and of the Federal Government are not growing in proportion to the rapidly evolving threat, we remain steadfast in our resolve to finds ways to work together better as a government, so that we may respond to cyber threats with agility, efficiency, persistence, and ferocity.

The FBI recognizes other agencies have technical expertise, tools, and capabilities to leverage as we work together against cyber adversaries, and is committed to working through challenges associated with sharing sensitive law enforcement information and intelligence with interagency partners. The FBI understands the importance of whole-of-government collaboration, and will continue to find ways to work with the interagency in responding to cyber incidents in a coordinated manner. Given the recent developments in structuring the Department of Defense to defend the Nation against cyber adversaries, the FBI is committed to finding ways to partner more closely with U.S. Cyber Command in its newly elevated role as a Unified Combatant Command and its Cyber Mission Force teams.

We at the FBI appreciate this committee's efforts in making cyber threats a focus and committing to improving how we can work together to better defend our nation against our increasingly capable and persistent adversaries. We look forward to discussing these issues in greater detail and answering any questions you may have.

Chairman MCCAIN. Thank you, Mr. Smith.

Mr. Krebs?

STATEMENT OF CHRISTOPHER C. KREBS, PERFORMING THE DUTIES OF THE UNDER SECRETARY FOR THE NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. KREBS. Chairman McCain, Ranking Member Reed, members of the committee, thank you for the opportunity to appear before you today.

In my current role performing the duties of the Under Secretary for the National Protection and Programs Directorate, I lead the Department of Homeland Security's efforts to secure and defend our federal networks and facilities, manage systemic risk to critical infrastructure, and improve cyber and physical security practices across our Nation.

This is a timely hearing as during October, we recognize National Cybersecurity Awareness Month, a time to focus on how cybersecurity is a shared responsibility that affects every business and organization in America. It is one of the most significant and strategic risks to the United States.

To address this risk as a Nation, we have worked together to develop the much needed policies, authorities, and capabilities across the interagency with State, local, and international partners in coordination with the private sector. The Department of Defense's Eligible Receiver exercise in 1997 laid bare our Nation's cybersecurity vulnerabilities and the related consequences, initiating a cross-government journey to respond to the growing cyber threat.

Over the ensuing 20 years, through a series of directives, executive orders, and other documents, culminating most recently with

Executive Order 13800, we have established an increasingly defined policy foundation for the cyber mission space.

Roles and responsibilities have been further bolstered by bipartisan legislation providing the executive branch, in particular DHS, much needed authorities to protect federal and critical infrastructure networks.

We can further solidify DHS' role by giving my organization a name that clearly reflects our operational mission, and I look forward to working with you in that effort.

Building on those policies and authorities, the Department continues to develop the operational capabilities to protect our networks. Today, the National Cybersecurity and Communications Integration Center, or NCCIC, is the center of gravity for DHS's cybersecurity operations. Here we monitor a federal-civilian enterprise-wide risk picture that allows us to manage risk across the .gov. More broadly, the NCCIC brings together our partners to share both classified and unclassified threat information and coordinate response efforts. Partners include representatives from the critical infrastructure community, State, local, tribal, and territorial governments, sector-specific liaisons from the Departments of Energy, Health and Human Services, Treasury, and Defense, intelligence community personnel, law enforcement partners such as the FBI, and liaisons from each of the cyber centers, including U.S. Cyber Command. They all sit with one another at the NCCIC.

We know that we cannot stop here and need to accelerate efforts to develop scalable solutions to manage systemic cybersecurity risks across the Nation's infrastructure.

Last year's Presidential Policy Directive 41, United States Cyber Incident Coordination, further clarified roles and set forth principles for the Federal Government's response to cyber incidents, including formalizing a cyber response group and cyber unified coordination group. It also required the Department to update the National Cyber Incident Response Plan, or NCIRP, which was completed last January.

Updating the NCIRP, in partnership with industry and State and local partners, was a critical step in cementing our shared responsibility and accomplished three main goals. First, it defines the role and responsibilities of all stakeholders during a cyber incident. Second, it identifies the capabilities required to respond to a significant cyber incident. Third, it describes the way our Federal Government will coordinate its activities with those affected by a cyber incident.

However, our focus going forward is to build on the NCIRP with multi-stakeholder operational plans and incident response playbooks, and then we must train and exercise to those plans in order to identify and address the seams and gaps that may exist.

We are building on our cyber mission workforce within the framework of the NCIRP with our hunt and incident response teams that exercise the tenets of the NCIRP each day. We work across the various stakeholders within the NCCIC to accomplish this mission.

In some cases, DHS teams are augmented with FBI and DOD personnel to provide a more robust and coordinated response. This

model of collaboration and cross-agency cooperation will continue taking advantage of the respective strengths of each agency.

To ensure we are focused on the mission that you, Congress, have tasked us with, we have prioritized filling all open cyber positions at DHS, cross training our workforce on instant response, and creating a cyber incident response surge capacity force modeled after FEMA's [Federal Emergency Management Agency] for natural disasters that can rise to meet any demand.

Before I close, I would like to add one last but critical element. The cyber defense mission is much broader than just response. It also encompasses preparedness and resilience, and we must continually assess and improve our cybersecurity posture against the latest threats, denying our adversaries opportunities to wreak havoc.

Finally, I would like to reinforce one more time we have made significant progress since Eligible Receiver, yet there is no question we have more to do. We must do it with a never-before-seen sense of urgency. By bringing together all stakeholders, we are taking action to manage cybersecurity risks, improve our whole-of-government incident response capabilities, and become more resilient.

I thank you for the opportunity to testify, and I look forward to any questions you may have.

[The prepared statement of Mr. Krebs follows:]

PREPARED STATEMENT BY CHRISTOPHER KREBS

Chairman McCain, Ranking Member Reed, and members of the Committee, thank you for the opportunity to be here today. In this month of October, we recognize National Cybersecurity Awareness Month, a time to focus on how cybersecurity is a shared responsibility that affects all Americans. The Department of Homeland Security (DHS) serves a critical role in safeguarding and securing cyberspace, a core homeland security mission.

The National Protection and Programs Directorate (NPPD) is responsible for protecting civilian Federal Government networks and collaborating with other federal agencies, as well as state, local, tribal, and territorial governments, and the private sector to defend against cyber threats. We endeavor to enhance cyber threat information-sharing across the globe to stop cyber incidents before they start and help businesses and government agencies to 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, we are taking action to protect against cybersecurity risks, improve our whole-of-government incident response capabilities, enhance information sharing on best practices and cyber threats, and to strengthen resilience.

THREATS

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. The past year has marked a turning point in the cyber domain, at least in the public consciousness. We have long been confronted with a myriad of attacks against our digital networks. But over the past year, Americans saw advanced persistent threat actors, including hackers, cyber criminals, and nation states, increase the frequency and sophistication of these attacks. Our adversaries have been developing and using advanced cyber capabilities to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democracy through attempts to manipulate elections.

Global cyber incidents, such as the "WannaCry" ransomware incident in May of this year and the "NotPetya" malware incident in June, 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, NPPD had already taken actions to help protect networks from similar types of attacks. Through requested vulnerability scanning, NPPD helped stakeholders identify vulnerabilities on their networks so they could be patched before incidents and attacks occur. Recognizing that not all users are

able to install patches immediately, NPPD shared additional mitigation guidance to assist network defenders. As the incidents unfolded, NPPD led the Federal Government's incident response efforts, working with our interagency partners, including providing situational awareness, information sharing, malware analysis, and technical assistance to affected entities.

Historically, cyber actors have strategically targeted critical infrastructure sectors including energy, financial services, critical manufacturing, water and wastewater, and others with various goals ranging from cyber espionage to developing the ability to disrupt critical services. In recent years, DHS has identified and responded to malware such as Black Energy and Havex which were specifically created to target industrial control systems, associated with critical infrastructure such as power plants and critical manufacturing. More recently, the discovery of CrashOverride malware, reportedly used against Ukrainian power infrastructure in 2016, highlights the increasing cyber threat to our infrastructure.

In one recent campaign, advanced persistent threat actors targeted the cyber infrastructure of entities within the energy, nuclear, critical manufacturing, and other critical infrastructure sectors since at least May 2017. In response, DHS led the asset response, providing on-site and remote assistance to impacted entities, help them evaluate the risk, and remediate the malicious actor presence. In addition, DHS, the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE) shared actionable analytic products with critical infrastructure owners and operators regarding this activity. This information provides network defenders with the information necessary to understand the adversary campaign and allows them to identify and reduce exposure to malicious activity. In addition, DHS has been working together with DOE to assess the preparedness of our electricity sector and strengthen our ability to respond to and recover from a prolonged power outage caused by a cyber incident.

RELATIONSHIP WITH THE DEPARTMENT OF DEFENSE AND INTELLIGENCE COMMUNITY

Responding to the full range of cyber threats facing government and critical infrastructure requires a whole-of-government, whole-of-nation effort. As it does with other stakeholders, DHS partners closely with the Department of Defense (DOD), FBI, and the intelligence community in carrying out its cybersecurity mission. DHS, FBI, DOD, and the intelligence community have multiple ongoing lines of effort. We continue to refine and mature planning to identify available resources and outline clear roles and responsibilities. We continue to focus on sharing cyber threat information relevant to defending against the most sophisticated malicious cyber actors. When appropriate, we can leverage existing authorities to provide technical assistance. In the event a significant cyber incident exhausts existing resources within DHS, DHS can leverage DOD resources, capabilities, and capacity to assist domestic response efforts under a well exercised mechanism—defense support of civil authorities. DHS and our partners also regularly participate in joint cyber exercises.

CYBERSECURITY PRIORITIES

Earlier this year, the President signed Executive Order (EO) 13800, *on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.* This EO set in motion a series of assessments and deliverables to understand how to improve our defenses and lower our risk to cyber threats. DHS has organized around these deliverables, working with federal and private sector partners to work through the range of actions included in the EO.

We are emphasizing the security of federal networks. Across the Federal Government, agencies have been implementing action plans to use the industry-standard Department of Commerce's National Institute of Standards and Technology Cybersecurity Framework. Agencies are reporting to DHS and the Office of Management and Budget (OMB) on their cybersecurity risk mitigation and acceptance choices. In coordination with OMB, DHS is evaluating the totality of these agency reports in order to comprehensively assess the adequacy of the Federal Government's overall cybersecurity risk management posture.

Although federal agencies have primary responsibility for their own cybersecurity, DHS, pursuant to its various authorities, provides a common set of security tools across the civilian executive branch and helps federal agencies manage their cyber risk. NPPD's assistance to federal agencies includes (1) providing tools to safeguard civilian executive branch networks through the National Cybersecurity Protection System (NCPS), which includes "Einstein", and the Continuous Diagnostics and Mitigation (CDM) programs, (2) measuring and motivating agencies to implement policies, directives, standards, and guidelines, (3) serving as a hub for information sharing and incident reporting, and (4) providing operational and technical assist-

ance, including threat information dissemination and risk and vulnerability assessments, as well as incident response services. NPPD's National Cybersecurity and Communications Integration Center (NCCIC) is the civilian government's hub for cybersecurity information sharing, asset incident response, and coordination for both critical infrastructure and the Federal Government.

Einstein refers to the suite of intrusion detection and prevention capabilities that protects agencies' unclassified networks at the perimeter of each agency. Einstein provides situational awareness of civilian executive branch network traffic, so threats detected at one agency are shared with all others providing agencies with information and capabilities to more effectively manage their cyber risk. The U.S. Government could not achieve such situational awareness through individual agency efforts alone.

Today, Einstein is a signature-based intrusion detection and prevention capability that takes action on known malicious activity. Leveraging existing investments in the Internet Service Provider "ISP" infrastructure, our non-signature based pilot efforts to move beyond current reliance on signatures are yielding positive results in the discovery of previously unidentified malicious activity. DHS is demonstrating the ability to capture data that can be rapidly analyzed for anomalous activity using technologies from commercial, government, and open sources. The pilot efforts are also defining the future operational needs for tactics, techniques, and procedures as well as the skill sets and personnel required to operationalize the non-signature based approach to cybersecurity.

State, local, tribal, and territorial governments are able to access intrusion detection and analysis services through the Multi-State Information Sharing and Analysis Center (MS–ISAC). MS–ISAC's service, called Albert, closely resembles some Einstein capabilities. While the current version of Albert cannot actively block known cyber threats, it does alert cybersecurity officials to an issue for further investigation. DHS worked closely with MS–ISAC to develop the program and considers MS–ISAC to be a principal conduit for sharing cybersecurity information with state and local governments.

Einstein, the Federal Government's tool to address perimeter security will not block every threat; therefore, it must be complemented with systems and tools working inside agency networks—as effective cybersecurity risk management requires a defense-in-depth strategy that cannot be achieved through only one type of tool. NPPD's CDM program provides cybersecurity tools and integration services to all participating agencies to enable them to improve their respective security postures by reducing the attack surface of their networks as well as providing DHS with enterprise-wide visibility through a common federal dashboard.

CDM is helping us achieve two major advances for federal cybersecurity. First, agencies are gaining visibility, often for the first time, into the extent of cybersecurity risks across their entire network. With enhanced visibility, they can prioritize the mitigation of identified issues based upon their relative importance. Second, with the summary-level agency-to-federal dashboard feeds, the NCCIC will be able to identify systemic risks across the civilian executive branch more effectively and closer to real-time. For example, the NCCIC currently tracks government-wide progress in implementing critical patches via agency self-reporting and manual data calls. CDM will transform this, enabling the NCCIC to immediately view the prevalence of a given software product or vulnerability across the Federal Government so that the NCCIC can provide agencies with timely guidance on their risk exposure and recommended mitigation steps. Effective cybersecurity requires a robust measurement regime, and robust measurement requires valid and timely data. CDM will provide this baseline of cybersecurity risk data to drive improvement across the civilian executive branch.

DHS conducts a number of activities to measure agencies' cybersecurity practices and works with agencies to improve risk management practices. The Federal Information Security Modernization Act of 2014 (FISMA) provided the Secretary of Homeland Security with the authority to develop and oversee implementation of Binding Operational Directives (BOD) to agencies. In 2016, the Secretary issued a BOD on securing High Value Assets (HVA), or those assets, federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. NPPD works with interagency partners to prioritize HVAs for assessment and remediation activities across the Federal Government. For instance, NPPD conducts security architecture reviews on these HVAs to help agencies assess their network architecture and configurations.

As part of the effort to secure HVAs, DHS conducts in-depth vulnerability assessments of prioritized agency HVAs to determine how an adversary could penetrate a system, move around an agency's network to access sensitive data, and exfiltrate such data without being detected. These assessments include services such as penetration testing, wireless security analysis, and "phishing" evaluations in which DHS hackers send emails to agency personnel and test whether recipients click on potentially malicious links. DHS has focused these assessments on federal systems that may be of particular interest to adversaries or support uniquely significant data or services. These assessments provide system owners with recommendations to address identified vulnerabilities. DHS provides these same assessments, on a voluntary basis upon request, to private sector and state, local, territorial, and tribal (SLTT) partners. DHS also works with the General Services Administration to ensure that contractors can provide assessments that align with our HVA initiative to agencies.

Another BOD issued by the Secretary directs civilian agencies to promptly patch known vulnerabilities on their Internet-facing systems that are most at risk from their exposure. The NCCIC conducts Cyber Hygiene scans to identify vulnerabilities in agencies' internet-accessible devices and provides mitigation recommendations. Agencies have responded quickly in implementing the Secretary's BOD and have sustained this progress. When the Secretary issued this directive, NPPD identified more than 360 "stale" critical vulnerabilities across federal civilian agencies, which means the vulnerabilities had been known for at least 30 days and remained unpatched. Since December 2015, NPPD has identified an average of less than 40 critical vulnerabilities at any given time, and agencies have addressed those vulnerabilities rapidly once they were identified. By conducting vulnerability assessments and security architecture reviews, NPPD is helping agencies find and fix vulnerabilities and secure their networks before an incident occurs.

In addition to efforts to protect government networks, EO 13800 continues to examine how the 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 are identifying authorities and capabilities that agencies could employ, soliciting input from the private sector, and developing recommendations to support the cybersecurity efforts of those critical infrastructure entities at greatest risk of attacks that could result in catastrophic impacts.

For instance, by sharing information quickly and widely, we help all partners block cyber threats before damaging incidents occur. Equally important, the information we receive from partners helps us identify emerging risks and develop effective protective measures.

Congress authorized the NCCIC as the civilian hub for sharing cyber threat indicators and defensive measures with and among federal and non-federal entities, including the private sector. As required by the Cybersecurity Act of 2015, we established a capability, known as Automated Indicator Sharing (AIS), to automate our sharing of cyber threat indicators in real-time. AIS protects the privacy and civil liberties of individuals by narrowly tailoring the information shared to that which is necessary to characterize identified cyber threats, consistent with longstanding DHS policy and the requirements of the Act. AIS is a part of the Department's effort to create an environment in which as soon as a company or federal agency observes an attempted compromise, the indicator is shared in real time with all of our partners, enabling them to protect themselves from that particular threat. This real-time sharing capability can limit the scalability of many attack techniques, thereby increasing the costs for adversaries and reducing the impact of malicious cyber activity. An ecosystem built around automated sharing and network defense-in-depth should enable organizations to detect and thwart the most common cyberattacks, freeing their cybersecurity staff to concentrate on the novel and sophisticated attacks. More than 129 agencies and private sector partners have connected to the AIS capability. Notably, partners such as information sharing and analysis organizations (ISAOs) and computer emergency response teams further share with or protect their customers and stakeholders, significantly expanding the impact of this capability. AIS is still a new capability and we expect the volume of threat indicators shared through this system to substantially increase as the technical standards, software, and hardware supporting the system continue to be refined and put into full production. As more indictors are shared from other federal agencies, SLTT governments, and the private sector, this information sharing environment will become more robust and effective.

Another part of the Department's overall information sharing effort is to provide federal network defenders with the necessary context regarding cyber threats to

prioritize their efforts and inform their decision making. DHS's Office of Intelligence and Analysis (I&A) has collocated analysts within the NCCIC responsible for continuously assessing the specific threats to federal networks using traditional all source methods and indicators of malicious activity so that the NCCIC can share with federal network defenders in collaboration with I&A. Analysts and personnel from the DOD, Energy, Treasury, Health and Human Services, FBI, and others are also collocated within the NCCIC and working together to understand the threats and share information with their sector stakeholders.

MITIGATING CYBER RISKS

We also continue to adapt to the evolving risks to critical infrastructure, and prioritize our services to mitigate those risks. Facing the threat of cyber-enabled operations by a foreign government during the 2016 elections, DHS and our interagency partners conducted unprecedented outreach and provided cybersecurity assistance to state and local election officials. Information shared with election officials included indicators of compromise, technical data, and best practices that have assisted officials with addressing threats and vulnerabilities related to election infrastructure. Through numerous efforts before and after Election Day, DHS and our interagency partners have declassified and publicly shared significant information related to the Russian malicious cyber activity. These steps have been critical to protecting our elections, enhancing awareness among election officials, and educating the American public. The designation of election infrastructure as critical infrastructure serves to institutionalize prioritized services, support, and provide data protections and does not subject any additional regulatory oversight or burdens.

As the sector-specific agency, NPPD is providing overall coordination guidance on election infrastructure matters to subsector stakeholders. As part of this process, the Election Infrastructure Subsector Government Coordinating Council (GCC) is being established. The Election Infrastructure Subsector GCC will be a representative council of federal, state, and local partners with the mission of focusing on sector-specific strategies and planning. This will include development of information sharing protocols and establishment of key working groups, among other priorities.

The Department also recently took action against specific products which present a risk to federal information systems. After careful consideration of available information and consultation with interagency partners, last month the Acting Secretary issued a BOD directing federal Executive Branch departments and agencies to take actions related to the use or presence of information security products, solutions, and services supplied directly or indirectly by AO Kaspersky Lab or related entities. The BOD calls on departments and agencies to identify any use or presence of Kaspersky products on their information systems in the next 30 days, to develop detailed plans to remove and discontinue present and future use of the products in the next 60 days, and at 90 days from the date of this directive, unless directed otherwise by DHS based on new information, to begin to implement the agency plans to discontinue use and remove the products from information systems. This action is based on the information security risks presented by the use of Kaspersky products on federal information systems.

The Department is providing an opportunity for Kaspersky to submit a written response addressing the Department's concerns or to mitigate those concerns. The Department wants to ensure that the company has a full opportunity to inform the Acting Secretary of any evidence, materials, or data that may be relevant. This opportunity is also available to any other entity that claims its commercial interests will be directly impacted by the directive.

CONCLUSION

In the face of increasingly sophisticated threats, NPPD stands on the front lines of the Federal Government's efforts to defend our nation's critical infrastructure from natural disasters, terrorism and adversarial threats, and technological risk such as those caused by cyber threats. Our infrastructure environment today is complex and dynamic with interdependencies that add to the challenge of securing and making it more resilient. Technological advances have introduced the "Internet of Things" (IOT) and cloud computing, offering increased access and streamlined efficiencies, while increasing our footprint of access points that could be leveraged by adversaries to gain unauthorized access to networks. As our nation continues to evolve and new threats emerge, we must integrate cyber and physical risk in order to understand how to effectively secure it. Expertise around cyber-physical risk and cross-sector critical infrastructure interdependencies is where NPPD brings unique expertise and capabilities.

We must ensure that NPPD is appropriately organized to address cybersecurity threats both now and in the future, and we appreciate this Committee's leadership in working to establish the Cybersecurity and Infrastructure Security Agency. As the Committee considers these issues, we are committed to working with Congress to ensure that this effort is done in a way that cultivates a safer, more secure and resilient Homeland.

Thank you for the opportunity to testify, and I look forward to any questions you may have.

Chairman MCCAIN. Thank you, Mr. Krebs. I thank the witnesses.

I am sure you can see that chart over there. Charts are always interesting, but this one we are going to need someone to translate for us because it is an example—and I think an accurate one—of the differences in authorities and responsibilities, none of which seem to have an overall coordinating office or individual. Of course, Mr. Joyce's absence here, whose job it is to do all this, is an example, frankly, of the disarray in which this whole issue rests.

Mr. Rapuano, to start with, you said that it is not the Department of Defense's responsibility. Suppose that the Russians had been able to affect the outcome of the last election. Would that not fall under the responsibility and authority, to some degree, of the Department of Defense, if they are able to destroy the fundamentals of democracy, which would be to change the outcome of an election?

Mr. RAPUANO. Mr. Chairman, specifically the issues associated with protecting elections from cyber incursion——

Chairman MCCAIN. So you are saying cyber incursion is not something that requires the Department of Defense to be engaged in. Is that correct?

Mr. RAPUANO. No, Mr. Chairman. I was simply saying that based on the State authorities and the State control of the election process in each State, there are issues associated with Federal authorities to engage.

Chairman MCCAIN. So those issues could be corrected by legislation. They are not engraved in tablets. Okay? So for you to sit there and say, well, but it is not the Department of Defense's responsibility, it is, to defend the Nation. The very fundamental, the reason why we are here is because of free and fair elections. If you can change the outcome of an election, that has consequences far more serious than a physical attack. So I am in fundamental disagreement with you about the requirements of the Department of Defense to defend the fundamental of this Nation, which is a free and fair election, which we all know the Russians tried to affect the outcome of. Whether they did or not is a matter of opinion. I do not think so.

But for you to shuffle off this, oh, well, it is not an attack, it is an attack of enormous proportions. If you can change the outcome of an election, then what is the Constitution and our way of life all about. I think Senator Rounds will be much more articulate on that issue.

So, one, I disagree with your assessment. One of the reasons why we have been so frustrated is exactly what you just said. It is exactly what you just said that, well, it is not the Department of Defense's job. It is the Department of Defense's job to defend this Nation. That is why it is called the Department of Defense.

Mr. Krebs, numerous experts over the past few years have highlighted the need for a dramatic change. According to the Presidential Commission on Enhancing National Cybersecurity, "The current leadership and organizational construct for cybersecurity within the Federal Government is not commensurate with the challenges of securing a digital economy and supporting the national economic security of the United States."

General Keith Alexander, one of the most respected men in the world, said before this full committee in March, "When we talk to the different agencies, they don't understand the roles and responsibilities. When you ask each of them who is defending what, you get a different answer."

Admiral Jim Stavridis: "There needs to be a voice in the cabinet that focuses on cyber."

Obviously, there is supposedly one there, but he is not appearing before this committee. That diminishes our ability to carry out our responsibilities.

The list goes on and on.

January 2017, the Center for Strategic and International Studies task force simply concluded, "We must consider how to organize the United States to defend cyberspace, and that if DHS is unable to step up its game, we should consider the creation of a new cybersecurity agency."

The list goes on and on.

I would like to have your responses to these assessments ranging from a presidential commission to General Keith Alexander to the Atlantic Council to the Center for Strategic and International Studies task force. All of them are saying the same thing, gentlemen. All of them are saying exactly the same thing. I look forward to getting a translator who can show us what this chart means. I will be glad to hear your responses. Secretary Rapuano?

Mr. RAPUANO. Mr. Chairman, I would say just on the issue of the election process, the Department is clearly there to support the response or the mitigation of potential threats to our electoral process. It is simply that when you look at the separation of authorities between State and local governments, the lead for that coordination and support in our current system is DHS. We provide defense support to civil authorities, as requested, to support those needs and requirements.

Chairman MCCAIN. That obviously assumes that the Department of Homeland Security has the capabilities and the authority in order to carry out that requirement, whereas this cyber is warfare. Cyber is warfare. Cyber is an attempt to destroy a democracy. That is what Mr. Putin is all about. So to somehow shuffle that off onto the Department of Homeland Security—of course, this goes back to this problem with this organizational chart. So I steadfastly reject your shuffling off the responsibilities of cyber over to the Department of Homeland Security. We have included in the NDAA [National Defense Authorization Act] a requirement for you to do so.

Mr. Smith, do you want to respond? Or Mr. Krebs?

Mr. KREBS. Sir, I am happy to.

Fundamentally this is a complex and challenging operational environment. Every one of the agencies represented here at the table

today, as you see in the bubble chart, as it is called, has a unique contribution across the ecosystem.

Chairman MCCAIN. Without coordination.

Mr. KREBS. Sir, I would suggest that we are getting there, that we are working on the coordination. PPD 41, the National Cyber Incident Response Plan, the cyber response group, and the cyber unified coordination group provide a foundation under which we can coordinate. We do work closely with Mr. Joyce and the National Security Council. However, from an operational perspective, I think the Department of Homeland Security and I in my role as Under Secretary have the direction and authorities I need to move out.

Now, the question is whether I have——

Chairman MCCAIN. Are we winning or losing?

Mr. KREBS. Sir, this is a battle that is going to be going on for many years. We are still trying to get our arms around it.

Chairman MCCAIN. I repeat my question. Are we winning or losing?

Mr. KREBS. Sir, it is hard to assess whether we are winning or losing. I would say that we are fighting this battle every day. We are working with the private sector. It is a complex environment, and I look forward to working with the Congress——

Chairman MCCAIN. Do you know that for 8 years we have been trying to get a policy? For 8 years, we have been trying to get a strategy. For 8 years, we have been trying to get something besides this convoluted chart. Do you know that?

Mr. KREBS. Yes, sir. I have been in my role for 8 weeks. I understand your frustration. I share your frustration. I think we have a lot of work to do, and I think this is going to require both the executive branch and the Congress working together to continue understanding exactly how we need to address the threat.

Chairman MCCAIN. Well, when a coordinator does not show up for a hearing, that is not an encouraging sign.

Senator Reed?

Senator NELSON. I wish you would consider a subpoena to get the main witness.

Chairman MCCAIN. I think that has to be discussed in the committee.

Senator REED. Well, thank you, Mr. Chairman.

Thank you, gentlemen, for your testimony.

The chairman has raised the issue of Russian involvement in our last election, but our intelligence community essentially assured us that they are going to come back with more brio, or whatever the right term is.

Have you been told to prepare for that, Mr. Rapuano? Has the Defense Department been given sort of the directions to coordinate, to take all steps advise the administration on what you can do to prevent, preempt, or to respond to a Russian intrusion in 2018?

Mr. RAPUANO. Senator, I am not aware of a specific direction in terms of a specific task associated with the election process. We are engaging on a routine basis with DHS and the rest of the interagency community to develop priorities and consider responses, as well as mitigation measures. As I tried to note earlier, the competing authorities associated with the electoral process really do

call for a thoughtful orchestration of how we would direct and task and engage with those State and local authorities. It really does need to be coordinated because each agency brings something different. There is a private sector component because most States get very significant support in terms of their electoral systems from private entities. So we are certainly engaged in the process, and we are certainly available to support——

Senator REED. But you have not been directed to start actively planning and coordinating with respect to the elections specifically.

Mr. RAPUANO. No, not to my knowledge, Senator.

Senator REED. Mr. Smith, have you in your agency, the FBI, been told to begin actively coordinating with respect to the 2018 election in terms of interrupting, preempting, and responding to Russian intrusions, which again the intelligence community practically assures this will happen?

Mr. SMITH. Yes, Senator.

Senator REED. You have been.

Mr. SMITH. Yes, sir.

Senator REED. Can you describe what you have been doing?

Mr. SMITH. Yes, sir.

Senator REED. In general terms.

Mr. SMITH. In general terms? Sir, we have not stopped since the last election coordinating and keeping together an election fusion cell, which is jointly located at the Hoover Building, and working with our interagency partners not only on what had transpired and getting deeper on that but also working forward as to what may come towards us in the upcoming midterms and 2018 election cycles. So we are actively engaged both with outreach in the communities and with the DHS and their election task force, along with every field office has a designated election crimes coordinator who is on the ground out there in the event of any information coming towards us or any incidents that we would need to be aware of and react to.

Senator REED. Thank you.

Mr. Krebs, the same question basically.

Mr. KREBS. Sir, absolutely. But I will tell you this. I did not need anybody to tell me to stand up a task force or anything like that. The first thing I did when I came in 8 weeks ago was assess the state of the election infrastructure activities underway at the Department of Homeland Security and establish an election security task force, which brings together all the components under me within NPPD [National Protection and Programs Directorate], but also works closely with the intelligence and analysis component within DHS, as well as the FBI and out other interagency partners.

I think we have made some progress here. I think there is a lot more to do, as Director Smith mentioned. We are not just thinking about 2018. We are thinking about the gubernatorial elections that are coming up in a matter of weeks. Just last week, we worked with 27 States, the Election Assistance Commission, and established the Government Coordinating Council, a body under which all the State election officials can come together and provide a foundation which coordinates security practices and shares information. We are issuing security clearances to a number of election officials, and, in a matter of weeks, we are going to establish a sec-

tor coordinating council, which will bring those private sector elements that provide the systems and technologies and support.

So I think there is still a lot to be done. We certainly have work ahead of us, and there is no question they are going to come back, and we are going to be fighting them every day. Yes, sir.

Senator REED. You mentioned several times the need to engage the private sector. That is a challenge. In fact, it might be more important in this context than in any other quasi-military context since they lead, whereas in other areas like missiles, bombers, and vehicles, it is the Government more than the private sector.

But just quickly, some of the things that we have to consider are sort of not this committee's responsibility but the legislation that Senator McCain and I are sponsoring for the SEC [Securities and Exchange Commission] so that they would have to designate if they have a cybersecurity expert on the board or why not is a way in which to disclose to shareholders but also to provide an incentive for them to be more keyed into cyber. There have been some discussions. I was talking to Mr. Rapuano about using TRIA, the Terrorism Reinsurance, as a way to incentivize. Without that, I do not think we are going to get the kind of buy-in.

So just very briefly because my time has expired, where are we in terms of private engagement? At the threshold or some engagement or it is still——

Mr. KREBS. Sir, I actually came out of the private sector. I spent the last several years at a major technology company where I managed a number of the cybersecurity policy issues. So I have a unique, I think, understanding of what it takes on the private sector side, as well as working in government.

We do have a number of private sector representatives within the NCCIC, and we have unique statutory authorities for coordinating with the critical infrastructure community.

There is a lot of work ahead of us. We need to better refine our value proposition, I think, to get more companies to come in and share information with us. But we do have a unique liability protection capability.

One thing that I think will certainly enable our advancement, as I mentioned in my opening, I need a name change. I need to be able to tell my stakeholders, my customers what it is I do. The National Protection and Programs Directorate does not tell you anything. I need something that says I do cybersecurity so I can go out there and I can clearly communicate what it is on a daily basis that I do. I think that is a big step forward.

Chairman MCCAIN. You tell us the title you want besides "President."

Senator REED. Yes. We will get you a T-shirt too.

[Laughter.]

Chairman MCCAIN. Senator Inhofe?

Senator INHOFE. Thank you, Mr. Chairman.

The three of you can relax because what I am going to address is to the empty chair. I know that this message will get through.

It has to do with section 881 and 886. They are some provisions in the Senate's version of the NDAA, specifically those sections, that have raised concerns among the software developers critical to our national defense. The purpose of these provisions are to make

available to the public the source code and proprietary data that is used by the Department of Defense.

Now, I would like to submit for the record numerous letters, which I will do in just a moment, and documents from the industry stakeholders that share my concerns with this language. While I understand the goals and intentions of the legislation, it creates some unintended consequences and impacts, such as limit the software choices available to DOD to serve the warfighter, increase costs to the Department of Defense by compromising the proprietary nature of software and limiting contractor options, and potentially aid U.S. adversaries and threaten DOD cybersecurity by sharing DOD's source code by placing it in a public repository, and also reducing competitiveness of American software and technology companies by opening the software contractor's intellectual property and code to the public repository.

As we progress into the conference report, I look forward to working with the Senate Armed Services Committee on a way forward on this topic and recommend that we study this issue prior to instituting new legislation. This is a provision that is in the Senate bill, not in the House bill.

I would ask unanimous consent to include in the record at this point, Mr. Chairman, these documents from the stakeholders.

Chairman MCCAIN. Without objection.

[The information follows:]

October 2, 2017

The Honorable John McCain
Chairman
Senate Armed Services Committee
228 Russell Senate Office Building
Washington, DC 20510

The Honorable Mac Thornberry
Chairman
House Armed Services Committee
2216 Rayburn House Office Building
Washington, DC 20515

The Honorable Jack Reed
Ranking Member
Senate Armed Services Committee
228 Russell Senate Office Building
Washington, DC 20510

The Honorable Adam Smith
Ranking Member
House Armed Services Committee
2216 Rayburn House Office Building
Washington, DC 20515

Re: Subtitle I of Title VIII of the National Defense Authorization Act for Fiscal Year 2018, H.R. 2810, as passed by Senate

Dear Chairmen McCain and Thornberry and Ranking Members Reed and Smith:

On behalf of the members of the Information Technology Alliance for Public Sector (ITAPS),[1] I am writing to share our opposition to the provisions of Subtitle I of Title VIII of the National Defense Authorization Act (NDAA) for Fiscal Year 2018, H.R. 2810, as passed by the Senate. After extensive discussions in the tech sector and with an increasingly larger cohort of solutions providers, developers of software and manufacturers of hardware containing firmware, there is extensive concern regarding the ramification of these proposals to past and future government acquisitions of software and firmware and we ask that the Subtitle be excluded from any final conference report.

Subtitle I, Sections 881 through 886 abruptly departs from current law by mandating government access to privately developed source code. These provisions are poorly drafted and create a disconnect in current law regarding the safeguarding of intellectual property rights of private companies on the one hand, and the requirement to hand over the most sacred of trade secrets for use by the government and its contractors, on the other hand. By turning the environment on its head, these changes could lead to a mass exodus of available contractors, diminishing the Department's ability to obtain the latest and most useful software products, and killing the small business retailers that contract to provide those products. Most importantly they will expose the Department to significant cybersecurity risk. In addition, sections in the subtitle would also retroactively alter the licensing of software already procured by the Department, without consideration for the terms and conditions under which the software was procured. Finally, theses sections seek to fundamentally alter the way the Department acquires, develops, procures, and implements major software systems through a significant expansion of government software development, replicating and competing with services and software now provided by a diverse,

[1] About ITAPS. ITAPS, a division of the Information Technology Industry Council (ITI), is an alliance of leading technology companies building and integrating the latest innovative technologies for the public sector market. With a focus on the federal, state, and local levels of government, as well as on educational institutions, ITAPS advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Visit itaps.itic.org to learn more. Follow us on Twitter @ITAlliancePS.

competitive domestic industrial base. For additional commentary on the individual provisions found in subtitle I, please see the attached appendix.

We disagree with the narrative that the Section 813 Panel is not addressing rights in technical data and intellectual property rights in software and firmware, and would encourage you to reach out Mr. Richard Ginman, Chair of the Panel, for discussions on how they have been wrangling with these issues over the last several years. While Congress has the authority to act on these matters, we believe that, because these issues have been the focus of the Panel, any legislative actions on these issues would be premature and undermine the work that the Department and stakeholders have invested in addressing these complicated issues.

Additionally, we are unable to resolve the requirements of the proposal to manage as open source software code that was delivered in current or previous contracts, as those include negotiated legal agreements about rights in technical data and ownership of intellectual property. Actions to publish the source code that was developed as part of these contracts would violate the business calculations those contractors and subcontractors used at the time the contracts were executed and potentially cause fatal harm to a host of American companies serving the defense industrial base.

Finally, because so much of the source code that would be subject to these provisions falls under the definition of commercial computer software as found at 48 CFR 2.101, and because of the limitations placed on the government use of that commercial computer software and firmware as outlined in DFARS 227.7202 and DFARS 227.7203-1, we believe that the issues and proposals raised as part of Sections 881 and 886 should be evaluated by the Section 813 Panel to allow for additional discussion.

Again, we appreciate the time and attention paid to our concerns and the willingness to address those concerns. At this time, we believe that striking the Subtitle is the only available recourse to resolve these issues and to allow the mechanisms already set in motion by the Congress on these topics to reach their completion.

We look forward to working with the Conferees as the bill advances, and we appreciate your attention to this letter. Should you have any questions or comments please contact Pam Walker at pwalker@itic.org.

Very respectfully,

APPENDIX: Commentary on Sections 881-886

SEC. 881 – RIGHTS IN TECHNICAL DATA

This section, which redefines "technical data" to include source code and the DOD's rights in technical data, would fundamentally alter long-standing rights of software companies to their intellectual property. First, unlike other portions of Title 10, Section 2320 and the Federal Acquisition Regulation (FAR) and the Defense FAR Supplement (DFARS)), the text does not appear to make a distinction between software developed at public expense for the government and that created outside of government programs by the private sector. Under current law, the Department receives limited rights to software provided to the government for its use, but developed independently by the private sector. By making this distinction, the entire law can be read consistently to preserve all intellectual property rights of each party – as is explicitly required by 10 U.S.C. § 2320(a)(1).

The proposed text requires that all "[s]oftware shall be delivered in native electronic format" to the Department, which would require commercial software companies to provide the source code of their products to DOD. The explanation given is that the Department would "make use of" the data "to develop, configure, adapt, or maintain its software assets." Such terms are unheard of in the software industry, and would severely undermine the intellectual property rights of DOD contractors. The proposed text would have disastrous consequences for the Department. Since a company's source code is its most valuable commodity, it is highly likely that software companies, particularly commercial software companies, will opt out of DOD work, thereby leaving the Department without some of its most critical partners that provide the most innovative, effective and secure products. If the Department is seeking additional information from its contractors, the Department should work with private industry to develop alternative ways for contractors to provide the Department the information and assurances that it actually needs without disregarding the intellectual property rights that drive American innovation.

Second, this provision would significantly weaken security for the US Government in that companies forced to hand over source code to DOD would, 1) be subject to greater security risks of a breach because the source code of all software products would then be centralized with the government; and 2) be subject to the expansion of this provision in every country in which they operate, including adversaries such as Russia and China. China has already actively sought access to source code for participation in its markets, but many technology companies have pushed back citing intellectual property laws and trade protections for IP. This provision, if enacted, would significantly undermine those protections.

SEC. 882 – DEFENSE INNOVATION BOARD ANALYSIS OF SOFTWARE ACQUISITION REGULATIONS

This provision would require the Defense Innovation Board to complete an analysis of software development and acquisition regulations for the Department of Defense. This work is already underway and being conducted by the panel created under Section 813 of the 2016 NDAA, and the DIB analysis is unnecessary and duplicative.

SEC. 883. PILOT TO TAILOR SOFTWARE INTENSIVE MAJOR PROGRAMS TO USE AGILE METHODS

This section directs the Secretary to conduct a pilot project in each service and one defense- wide program. Each pilot project would take an existing major defense acquisition program and alter the way the program is being conducted so as to employ an "Agile" framework which would fundamentally change the project's existing program business plan. Furthermore, it provides for termination of existing vendors who cannot alter already negotiated and accepted terms and conditions that do not meet the new framework. This strong-arm tactic will signal to industry an anti-business approach by the DOD, which may cause otherwise interested contractors from doing business with the Department, thereby leaving it with fewer technology choices and limiting competitive bidding. Finally, the language limits the entities who can compete for this work to government entities, or federally funded research and development centers; there are no provisions for including the private sector in what amounts to major changes to existing projects. Competition, a fundamental principle under the FAR, isn't even a consideration for these pilot programs.

SEC. 884. REVIEW AND REALIGNMENT OF DEFENSE BUSINESS SYSTEMS TO EMPHASIZE AGILE METHODS

In much the same way as section 883 focuses on pilot projects, section 884 attempts to apply the "Agile" framework and limited competition to existing business system projects. This section uses much of the same language of section 883 and again violates existing terms and conditions of previously agreed to contracts, eliminates competition and directs work to FFRDC's and government digital services entities such as USDS and GSA's 18f. Similar to Sec. 883, this provision specifically requires the DOD to consider terminating contractors that are unwilling to meet the demands of this section. Again, these strong-arm tactics in dealing with contracting partners will only drive away contractors making the DOD less effective as it will not have access to the full breadth of technology contracting community.

SEC. 885. SOFTWARE DEVELOPMENT PILOT USING AGILE BEST PRACTICES.

Section 885 mirrors sections 883 and 884 in that it attempts to apply a new framework for development of four to eight software development pilot projects at DOD. All software developed under this section must be open source, but the type of open source license is not defined. This section also uses similar language to eliminate competition and direct work to FFRDC's and government digital services entities such as USDS and GSA's 18F.

SEC. 886. USE OF OPEN SOURCE SOFTWARE.

This section mandates that all unclassified custom-developed computer software developed for DOD 180 days after enactment shall be managed as open source software unless specifically waived by the service acquisition executive. It further requires the Secretary to release all source code to a public repository "available to anyone for any purpose." The section goes on to direct the Secretary to "apply open source licenses to existing custom-developed computer software; and release related source code and technical data in a public repository location approved by the Department of Defense." The cyber security risks in these actions are legion. Providing Source Code on DOD applications for review and testing in a public repository, not to mention providing a forum for submission of changes to that code by outside entities, presents adversaries with a tremendous gateway to DOD technology assets. The final language of section 886, which

was modified by an adopted amendment to exclude Commercial Off the Shelf Software, would not protect the intellectual property of companies whose products are commercially available, but not sold on the shelf to the general public. This would logically deter these companies, both large and small, from working with defense contractors to develop solutions vital to our national security. Furthermore, publishing the source code of legacy applications, many of which are meant to be operated in a secure environment with restricted access, versus being exposed to the Internet, will allow adversaries to exploit weaknesses in code on production systems.

S. 1519 NDAA – Concerns with Subtitle I – Development and Acquisition of Software Intensive And Digital Products and Services

Subtitle I, Sections 881 through 886 abruptly departs from current law by mandating government access to privately developed source code. These provisions are poorly drafted and create a disconnect in current law regarding the safeguarding of intellectual property rights of private companies on the one hand, and the requirement to hand over the most sacred of trade secrets for use by the government and its contractors, on the other hand. By turning the environment on its head, these changes could lead to a mass exodus of available contractors, diminishing the Department's ability to obtain the latest and most useful software products, and killing the small business retailers that contract to provide those products. Most importantly they will expose the Department to significant cyber security risk. In addition, sections in the subtitle would also retroactively alter the licensing of software already procured by the Department without consideration for the terms and conditions under which the software was procured. Finally, theses sections seek to fundamentally alter the way the Department acquires, develops, procures, and implements major software systems through a significant expansion of government software development, replicating and competing with services and software now provided by a diverse, competitive domestic industry.

SEC. 881 – RIGHTS IN TECHNICAL DATA

This section, which redefines "technical data" to include source code and the DOD's rights in technical data, would fundamentally alter long-standing rights of software companies to their intellectual property. First, unlike other portions of Title 10, Section 2320 and the Federal Acquisition Regulation (FAR) and the Defense FAR Supplement (DFARS)), the text does not appear to make a distinction between software developed at public expense for the government and that created outside of government programs by the private sector. Under current law, the Department receives limited rights to software provided to the government for its use, but developed independently by the private sector. By making this distinction, the entire law can be read consistently to preserve all intellectual property rights of each party – as is explicitly required by 10 U.S.C. § 2320(a)(1).

The proposed text requires that all "[s]oftware shall be ***delivered*** in native electronic format" to the Department, which would require commercial software companies to provide the source code of their products to DOD. The explanation given is that the Department would "make use of" the data "to develop, configure, adapt, or maintain its software assets." Such terms are unheard of in the software industry, and would severely undermine the intellectual property rights of DOD contractors.

The proposed text would have disastrous consequences for the Department. Since a company's source code is its most valuable commodity, it is highly likely that software companies, particularly commercial software companies, will opt out of DOD work, thereby leaving the Department without some of its most critical partners that provide the most innovative, effective and secure products. If the Department is seeking additional information from its contractors, the Department should work with private industry to develop alternative ways for contractors to provide the Department the information and assurances that it actually needs without disregarding the intellectual property rights that drive American innovation.

Second, this provision would significantly weaken security for the US Government in that companies forced to hand over source code to DOD would, 1) be subject to greater security risks of a breach because the source code of all software products would then be centralized with the government; and 2) be subject to the expansion of this provision in every country in which they operate, including adversaries such as Russia and China. China has already actively sought access to source code for participation in its markets, but many technology companies have pushed back citing intellectual property laws and trade protections for IP. This provision, if enacted, would significantly undermine those protections.

SEC. 882 – DEFENSE INNOVATION BOARD ANALYSIS OF SOFTWARE ACQUISITION REGULATIONS

This provision would require the Defense Innovation Board to complete an analysis of software development and acquisition regulations for the Department of Defense. This work is already underway and being conducted by the panel created under Section 813 of the 2016 NDAA, and the DIB analysis is unnecessary and duplicative.

SEC. 883. PILOT TO TAILOR SOFTWARE INTENSIVE MAJOR PROGRAMS TO USE AGILE METHODS

This section directs the Secretary to conduct a pilot project in each service and one defense-wide program. Each pilot project would take an existing major defense acquisition program and alter the way the program is being conducted so as to employ an "Agile" framework which would fundamentally change the project's existing program business plan. Furthermore, it provides for termination of existing vendors who cannot alter already negotiated and accepted terms and conditions that do not meet the new framework. This strong-arm tactic will signal to industry an anti-business approach by the DOD, which may cause otherwise interested contractors from doing business with the Department, thereby leaving it with fewer technology choices and limiting competitive bidding. Finally, the language limits the entities who can compete for this work to government entities, or federally funded research and development centers; there are no provisions for including the private sector in what amounts to major changes to existing projects. Competition, a fundamental principle under the FAR, isn't even a consideration for these pilot programs.

SEC. 884. REVIEW AND REALIGNMENT OF DEFENSE BUSINESS SYSTEMS TO EMPHASIZE AGILE METHODS

In much the same way as section 883 focuses on pilot projects, section 884 attempts to apply the "Agile" framework and limited competition to existing business system projects. This section uses much of the same language of section 883 and again violates existing terms and conditions of previously agreed to contracts, eliminates competition and directs work to FFRDC's and government digital services entities such as USDS and GSA's 18f. Similar to Sec. 883, this provision specifically requires the DOD to consider terminating contractors that are unwilling to meet the demands of this section. Again, these strong-arm tactics in dealing with contracting partners will only drive away contractors making the DOD less effective as it will not have access to the full breadth of technology contracting community.

SEC. 885. SOFTWARE DEVELOPMENT PILOT USING AGILE BEST PRACTICES.

Section 885 mirrors sections 883 and 884 in that it attempts to apply a new framework for development of four to eight software development pilot projects at DOD. All software developed under this section must be open source, but the type of open source license is not defined. This section also uses similar language to eliminate competition and direct work to FFRDC's and government digital services entities such as USDS and GSA's 18f.

SEC. 886. USE OF OPEN SOURCE SOFTWARE.

This section mandates that all unclassified custom-developed computer software developed for DOD 180 days after enactment shall be managed as open source software unless specifically waived by the service acquisition executive. It further requires the Secretary to release all source code to a public repository "available to anyone for any purpose." The section goes on to direct the Secretary to "apply open source licenses to existing custom-developed computer software; and release related source code and technical data in a public repository location approved by the Department of Defense."

The cyber security risks in these actions are legion. Providing Source Code on DOD applications for review and testing in a public repository, not to mention providing a forum for submission of changes to that code by outside entities, presents adversaries with a tremendous gateway to DOD technology assets. Furthermore, publishing the source code of legacy applications, many of which are meant to be operated in a secure environment with restricted access, versus being exposed to the Internet, will allow adversaries to exploit weaknesses in code on production systems.

We strongly recommend the removal of subsection I and sections 881 – 886 from S. 1519 the National Defense Authorization Act. The legislation provides no justification for this fundamental shift in policy, and this strategy is contrary to our national security interests with no discernible benefit to the Department.

TECHNET
THE VOICE OF THE INNOVATION ECONOMY

805 15th Street, NW, Suite 708, Washington, D.C. 20005
Telephone 202.650.5100 | Fax 202.650.5118
www.technet.org | @TechNetUpdate

October 2, 2017

Senator John McCain
Chairman
Senate Armed Services Committee
228 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Mac Thornberry
Chairman
House Armed Services Committee
2216 Rayburn House Office Building
Washington, D.C. 20515

Senator Jack Reed
Ranking Member
Senate Armed Services Committee
228 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Adam Smith
Ranking Member
House Armed Services Committee
2216 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairmen McCain and Thornberry and Ranking Members Reed and Smith:

TechNet is the national, bipartisan network of innovation economy CEOs and senior executives. Our diverse membership includes dynamic startups and the most iconic companies on the planet and represents more than 2.7 million employees in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, biotechnology, venture capital, and finance.

We appreciate your commitment to America's national defense and to advancing policies in the 2018 *National Defense Authorization Act* (NDAA) that enable our nation's technology sector to continue partnering with the Department of Defense to produce technological solutions that protect Americans and our allies in a fiscally responsible manner.

I am writing regarding concerns raised within our industry about Subtitle I, Sections 881-886 of the NDAA that recently passed in the U.S. Senate's version of the NDAA (S. 1519). We are concerned that this proposal could force commercial enterprises partnering with the Department of Defense to publicly share their intellectual property — specifically their proprietary source code — as a condition of doing business with the government in procurement contracting.

For years, there has been broad bipartisan consensus around the idea that Americans' intellectual property must be carefully protected. Proprietary source code is a key form of intellectual property that drives computer programs and software. At both the state and federal levels, TechNet has opposed government

efforts to force technology manufacturers to reveal their proprietary source code due to increased cybersecurity risks.

We fear that forcing technology companies to open up their intellectual property to the public, including our nation's adversaries, could create significant security vulnerabilities. This section's call for the Department of Defense to create a "repository" for housing its newly acquired source code is also concerning, as it would become a prime target for cybercriminals at a time when our federal government's information technology infrastructure remains in desperate need of full-scale modernization as envisioned under the *Modernizing Government Technology Act*. Additionally, we have opposed China's cybersecurity law on the basis of its call for forced technology transfers. We are concerned that adopting this policy in the NDAA could embolden America's adversaries to pursue similar concessions from U.S. innovators as a condition of our commercial relationships, in addition to weakening our competitive advantage.

From an economic standpoint, TechNet has long advocated for policies that protect the ideas of American innovators from intellectual property theft, including protections for proprietary source code. At the state level, we have opposed measures forcing technology manufacturers to reveal their proprietary source code. In the context of international commerce, we have insisted that these proprietary source code protections be a key part of all trade agreements, including the current effort to modernize the North American Free Trade Agreement (NAFTA). Should this section of the NDAA become law, it would send a message to our trading partners that the U.S. is willing to accept weakened proprietary source code protections as part of a negotiation.

Finally, one of TechNet's top priorities is to fully equip our federal government with the tools necessary to modernize our information technology systems using existing commercial technologies that are constantly tested and improved to provide superior capabilities, stay ahead of cybercriminals, and avoid wasteful government spending. We are concerned that sections 881-886 of the Senate's NDAA create a preference for open-source technology only, and that the section encourages government entities — such as the U.S. Digital Service and the 18F office within the General Services Administration — to develop more customized code. By creating a non-commercial preference, we believe this section could further encourage the Department of Defense to develop more unnecessary government-unique solutions, instead of adhering to existing commercial item preference laws that are designed to avoid the unnecessary waste of taxpayer dollars. Instead, we continue to encourage the Department of Defense to leverage all existing commercial technologies and best practices in order to effectively meet mission needs.

In sum, adopting a policy of forced proprietary source code transfers, technology preferences, restrictive development, and non-commercial item preferences could have broader implications to our cybersecurity and economic well-being that go well

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

beyond the Department of Defense. As the House and Senate prepare for a conference committee on the NDAA, we respectfully urge that Sections 881-886 be removed until they can receive further examination with input from the multiple committees that would have jurisdiction over these critical issues.

Sincerely,

Linda Moore
President & CEO

















September 18, 2017

Dear Senator,

On behalf of the undersigned organizations, we urge you to strike sections 881, 883, 884, 885, and 886 from S. 1519, the 2018 National Defense Authorization Act (NDAA). We believe these provisions would harm taxpayers by promoting costly sole-source, government-based technology concepts over proven private sector solutions; and violating long-standing technology neutral procurement policies. They would also adversely impact intellectual property rights and national security.

Title VIII, Subtitle I, "Development and Acquisition of Software Intensive and Digital Products and Services" is intended to improve information technology procurement at the Department of Defense (DOD). However, the language in Section 881 fundamentally violates U.S. copyright laws, as well as the Trade Secrets Act, by requiring companies providing software to the DOD to turn over source code in its native electronic format to the agency. The language of section 881 would also apply to commercial off-the-shelf (COTS) products. Taking such a drastic step as Section 881 contemplates, with virtually no debate, could have grave consequences for the innovation economy.

Section 883 specifies how IT projects within the DOD should be analyzed, designed, and procured. This section directs all software projects currently being developed, but considered as "at risk," to be procured through the General Services Administration's (GSA) Technology Transition Service, Office of 18F, even if a similar tool or resource might be available through the private sector. The GSA Office of Inspector General issued reports on October 24, 2016, and February 21, 2017, that identified wasteful spending and security issues surrounding the development of software products by 18F. It is therefore ironic that more "at risk" projects would fall under the auspices of an agency whose fiscal behavior is, in itself, risky.

The Office of 18F was started in March 2014 by a group of Presidential Innovation Fellows (established under former President Obama in 2012) to supposedly help improve and modernize government technology. It is simply not credible to believe that this fledgling operation with approximately 200 employees scattered throughout the U.S. can possibly provide better software for the DOD than long-established private sector companies with tens of thousands of employees (not to mention up-and-coming innovator firms that don't enjoy the subsidies provided to 18F). Regardless of the level of expertise of any federal operation, there should always be competition in the procurement process, particularly for the DOD.

Sections 884 and 885 specify the development practice commonly called "agile" as the preferred method for developing and/or acquiring information technology for the federal government. Codifying this method of development precludes the use of future practices that may be cost-effective or efficient improvements on this process.

Section 886 mandates that the DOD use open source for all future unclassified custom-developed software and related technical data that is not a defense article regulated pursuant to section 38 of the Arms Export Control Act. It is not a coincidence that 18F only uses open source software. Section 886 would expose the source code for numerous DOD applications to foreign entities. The Government Accountability Office has

designated the security of federal cyber assets as "high risk" for 20 years. Policymakers should bear this in mind before exposing critical national security systems to Section 886.

In 2004, the Office of Management and Budget issued guidance that required federal software purchases to be technology neutral. Section 886 violates this long-standing practice, and sets a precedent that could lead to establishing open source as the sole form of software to be used throughout the government. Congress should not effectively close DOD to any software option that might better serve taxpayers.

The problematic provisions in S. 1519 regarding IT procurement and intellectual property rights threaten great harm. To avoid this monumental mistake, Congress must act now by striking sections 881, 883, 884, 885, and 886 from S. 1519.
Sincerely,

Thomas A. Schatz
President
Council for Citizens Against Government Waste

Pete Sepp
President
National Taxpayer's Union

Andrew Langer
President
Institute for Liberty

John M. Palatiello
President
Business Coalition for Fair Competition (BCFC)

Grover Norquist
President
Americans for Tax Reform

Katie McAuliffe
Executive Director
Digital Liberty

David Williams
President
Taxpayers Protection Alliance

Daniel Schnieder
Executive Director
American Conservative Union

Senator INHOFE. Thank you.

Chairman MCCAIN. Senator Nelson?

Senator NELSON. Well, I would not exactly say that the three of you should relax, but I will address more directly not only to the empty chair but to General McMaster, to General Kelly, to the Vice President, and to the President. Did you realize that you handed out a chart that is 5 years old? The date on this chart is January of 2013. I mean, why in the world?

By the way, Senator Rounds is acknowledging this, and I want to say what a pleasure it has been to deal with Senator Rounds as the two leaders of the cyber subcommittee. I can tell you we are alarmed. You heard the alarm in the voice of the chairman.

Can we stipulate here that State election apparatuses, State election databases—can we stipulate that that is critical infrastructure?

Mr. KREBS. Sir, the Department of Homeland Security has made that designation.

Senator NELSON. Good.

Mr. KREBS. I have an election infrastructure subsection, sir.

Senator NELSON. Good. Therefore, a tampering or a changing or an interfering with State election databases being critical infrastructure would, in fact, be an attack upon our country. Can we stipulate that that would be the case?

Why is there silence?

Chairman MCCAIN. Let the record show there was silence.

Senator NELSON. Wow.

So do you realize that you can change——

Chairman MCCAIN. Could I just——

Senator NELSON. Please.

Chairman MCCAIN. In deference to the witnesses, they are not the ones who——

Senator NELSON. I understand. That is why I am referring my comments not only to the empty chair but to the people behind that empty chair, which is the National Security Council Advisor, General McMaster, the fellow who runs the White House staff, General Kelly, both of whom I have the highest respect and esteem for, and ultimately the Vice President and the President.

I would go back and listen. I would defer to the intensity of the chairman's remarks both in his opening remarks and his questions. You mess around with our election apparatus, and it is an attack on our country.

So let me give you an example. It does not even have to be that the Russians come in or the Chinese or some third party that is not a nation state. We already know that they are in 20 of our States. We know that from the reports that have been in the newspaper from the intelligence community. All you have to do is go into certain precincts. You do not even have to change the outcome of the actual vote count. You could just eliminate every 10th registered voter. So when Mr. Jones shows up on election day to vote, I am sorry, Mr. Jones, you are not a registered voter. You multiply that every 10th voter, you have got absolute chaos in the election. On top of it, you have the long lines that result, and as a result of that, people are discouraged from voting because they cannot wait in the long line and so forth and so on.

Now, this is the ultimate threat. I have said so many times in this committee Vladimir Putin cannot beat us on the land, in the air, on the sea, under the sea, or in space, but he can beat us in cyber. To hand out a 5-year-old dated chart as to how we are going to fix this situation just is totally, totally insufficient.

I rest my case, Mr. Chairman. I wish you would consider a subpoena.

Chairman MCCAIN. Would the witnesses desire to respond to that diatribe?

Senator NELSON. That eloquent diatribe.

[Laughter.]

Chairman MCCAIN. One of the most historic statements in the history of this committee.

[Laughter.]

Chairman MCCAIN. Go ahead, please.

Mr. RAPUANO. Mr. Chairman, I would say just in terms of the Department of Defense's role, it is important to note that the National Guard in a number of States, on the authority of the Governors, trained cyber-capable forces are assisting those States, and they are addressing, identifying vulnerabilities, and mitigating those vulnerabilities. Elements of them are part of the Cyber Mission Force, and we certainly view quite appropriate the Governor tasking them under State authority versus the Department of Defense attempting to insert itself into a process without directly being requested.

Chairman MCCAIN. Could I just say, sir, again we are appreciative of what the Guard is doing. We are appreciative of what local authorities are doing. We are appreciative of what all these different agencies are doing. But we see no coordination and no policy and no strategy. When you are ready to give that to us, we would be eager to hear about it.

Senator Fischer?

Senator FISCHER. Thank you, Mr. Chairman. Those are hard acts to follow—your diatribes.

But I would like to focus on something else now with regard to response. Gentlemen, one of the things that Admiral Rogers has emphasized is the need to move quicker across the board and faster threat detection, faster decision-making, and faster responses.

Mr. Krebs, can you walk us through the process by which an organization, an operator of a piece of critical infrastructure, for example, would reach out to you for help? I know they first have to detect the threat, and that can take some time. But what does the process look like once they contact you? How long does it take to begin working with them, and are there legal agreements that must be in place before a response team could operate on their network?

Mr. KREBS. Ma'am, thank you for the question.

There are, of course, a number of ways that a victim can discover they have been breached or they have some sort of intrusion. That is working whether with the intelligence community or the FBI can notify them or the Department of Homeland Security could inform them, or of course, one of their private sector vendors could discover an actor on their networks.

Now, how they reach out, there are a number of ways as well they can reach out. They can email us. They can call us. We have local official cybersecurity advisors throughout the region. We have protective security advisors throughout the region. They could also contact the FBI.

Once we are aware of an incident, we will then do an intake process. Every incident is going to be different. That is kind of a truism here. Every incident could be different.

In terms of timing, it all does depend on what the situation is, what kind of information they want to provide. We do have to work through a legal agreement just to, for instance, get on their networks and install government equipment and take a look. That can take time. It can depend, of course, on the legal back and forth as hours or even days. But I would view this as kind of an elastic spectrum. It could take—we are talking hours. It could take a couple days to a week. It all, of course, depends on the nature of the breach.

Senator FISCHER. If you determine that DOD has to be involved in the response as part of that team, I assume that is going to take more time then. That decision currently rests with the President. Is that correct?

Mr. KREBS. Ma'am, actually we do a fair amount of coordination with the Department of Defense. In fact, we do a cross-training on incident response matters. As I mentioned before, we do have blended teams that go out to the field for investigations that can be FBI or DOD assets.

In terms of the decision-making process, we do have agreements in place. We have an understanding in place that we do not necessarily have to go to the President. We do not actually have to go to the Secretary level. There are sub-level understandings that we are able to use each other's resources.

Senator FISCHER. Those agreements would also cover what types of military assistance that is going to be needed?

Mr. KREBS. It is a support function, but we are typically talking personnel.

Senator FISCHER. Mr. Rapuano, are the concepts of operations that define the specific requirements that DOD forces could be asked to fulfill and prioritize its assets or sectors that should be defended from cyber attack if we were going to have a high-end conflict?

Mr. RAPUANO. Senator, the focus of the domestic response capabilities, defense support to civil authorities when it comes to cyber, are those protection teams out of the Cyber Mission Force. Those are skilled practitioners who understand the forensics issues, the identification of the challenges of types of malware and different approaches to removing the malware from the systems.

As Mr. Krebs noted, the DSCA process, Defense Support to Civil Authorities, is a direct request for assistance from DHS to the Department, and we have authorities all the way down to COCOM [Combatant Command] commanders, specifically Cyber Command. Admiral Rogers has the authority in a number of areas to directly task those assets. It then comes up to me, and for certain areas, the Secretary—it requires his approval. But most of these things can be done at lower levels, and we have provided that assistance previously to DHS.

Senator FISCHER. So do you have that policy guidance in place? If there is a high-end conflict, it is a first come, first served? Do you have a way that you can prioritize how you are going to respond? Is that in place now?

Mr. RAPUANO. Absolutely. So a high-end conflict for which we are receiving cyber attacks and threats in terms of against our capabilities to project power, for example, would be an utmost priority for the Department, as well as attacks against the DOD information system. If we cannot communicate internally, we cannot defend the Nation. So those are the equivalent of heart, brain, lung function DOD equities and capabilities that we prioritize. We have resources that are available unless tapped by those uppermost priorities, and then it becomes hard decision times in terms of do we apply assets for domestic and critical infrastructure protection, for example, or to protection of the DODIN [Department of Defense Information Network] or other DOD capabilities.

Senator FISCHER. Thank you.

Senator REED [presiding]. On behalf of Chairman McCain, let me recognize Senator Shaheen.

Senator SHAHEEN. Thank you, Senator Reed.

Thank you to all of our witnesses for being here this morning.

I share the frustration that you are hearing from everyone on this committee about decisions that have not been made actually with respect to cyber threats affecting our Nation.

One example is the use of Kaspersky Lab's antivirus software on U.S. Government systems. Kaspersky Lab has reported links to Russian intelligence, and it is based in Moscow, subjects client data to the Kremlin's intrusive surveillance and interception laws. We just had a recent report of Kaspersky's role in a successful Russian cyber operation to steal classified information from an NSA employee's home computer. They remained on the list of approved software for way too long.

Now, this committee put an amendment in the NDAA that would have prohibited the use of that software by the Department of Defense. I am pleased that finally we have seen the administration act on that.

But I think it really raises the question of how we got to this point. So what standards were used in approving Kaspersky Lab as an appropriate choice to fill the U.S. Government's antivirus protection needs? Does the Government vet the origins and foreign business dealings of cybersecurity firms and software companies before these products are used in our systems? Are companies looking to contract with the U.S. Government required to disclose all their foreign subcontractors, as well as their work and dealings with foreign governments who may be a threat to the United States?

So I will throw those questions out to whoever would like to answer them.

Mr. KREBS. Ma'am, thank you for the question.

As you know, the binding operational directive that we issued several weeks ago, just over a month now, 30 some odd days ago, require federal civilian agencies to identify Kaspersky products if they have then and a plan to implement in over 90 days.

So what that tells me is that we still have a lot of work to do in terms of the processes that are in place to assess technology products that are on the civilian——

Senator SHAHEEN. I agree, and that is why I am asking those questions. I do not mean to interrupt, but I have limited time. What I would really like to know is what you can tell me about what standards we use, how do we vet those kinds of products, and how do we ensure that we do not have another case of Kaspersky being used in our sensitive government systems.

Mr. KREBS. If I may suggest, I would like to come back with the General Services Administration to take a look at that with you, and I will give you a more detailed briefing on how we do that.

Senator SHAHEEN. Thank you. I would appreciate that.

Also, Mr. Rapuano, I appreciate your taking some time this morning to spend a few minutes with me to talk about the Hewlett-Packard Enterprise which allowed a Russian defense agency to review the source code of software used to guard the Pentagon's classified information exchange network. Can you tell me: is the disclosure of our source codes to other entities a usual way of doing business? How did that happen?

Mr. RAPUANO. Senator, the details on that—as I shared with you this morning, we are working that. Our CIO [Chief Information Officer] is leading that effort with HPE on ArcSight. I can get you additional details with regard to our procedures. We have a layered

approach to defense of the DODIN. But we can follow up with those details for you.

Senator SHAHEEN. Well, thank you. I appreciate that. That was a rhetorical question to raise the point again that I have serious concerns about the attention that we are paying to these kinds of issues.

In April, DOD's logistics agency said that "HP ArcSight software and hardware are so embedded" that it could not consider other competitors'—"absence and overhaul of the current IT infrastructure." Do you believe that that is what is required? How are we ever going to address any of these problems if we say we cannot take action because it would create a problem in responding throughout other areas where we do business?"

Again, I appreciate that you are going to respond to the concerns that I laid out, including that one, at a later time.

I am almost out of time, but I just had one question for you, Mr. Krebs. That is, on this notice of this hearing, you are listed as performing the duties of the Under Secretary for the National Protection and Programs Directorate. You said you have been on the job for 8 weeks. What does that mean?

Mr. KREBS. Yes, ma'am. Thank you for the question.

I have actually been with the Department since March 2017 where I was a senior counselor to General Kelly. He moved to the White House, of course. Soon after that, I was appointed by the President to be the Assistant Secretary for Infrastructure Protection. In the meantime, we do have an open vacancy at the Under Secretary position. So as the senior official within the National Protection and Programs Directorate, I am the senior official performing the duties of the Under Secretary.

Senator SHAHEEN. Okay. So tell me what your current title is, in addition to having that as part of your responsibilities.

Mr. KREBS. The senior official performing the duties of the Under Secretary——

Senator SHAHEEN. No, no, no. I know that is what is on here. What is your actual title?

Mr. KREBS. Assistant Secretary for Infrastructure Protection. That is what I have been appointed. Yes, ma'am.

Senator SHAHEEN. Thank you, Mr. Chairman.

Chairman MCCAIN [presiding]. Thank you.

Senator Rounds, I want to thank you and Senator Nelson for the outstanding work you are doing on the cyber subcommittee. It has been incredibly important and very helpful. Thank you.

Senator ROUNDS. Thank you, Mr. Chairman. Let me just share with you my appreciation for you and the ranking member for elevating this particular discussion to the full committee status. Senator Nelson has been great to work with, and I appreciate the bipartisan way in which he has approached this issue.

I wish we had the same type of cooperation this morning with Mr. Joyce coming to visit with us. I personally did not see this as an adversarial discussion today. I saw this as one in which we could begin in a cooperative effort the discussion about how we take care of the seams that actually exist between the different agencies responsible for the protection of the cyber systems within our country.

I just wanted to kind of bring this out. This particular chart—I believe General Alexander indicated that there were 75 different revisions to this particular chart when it was created. Let me just, to clear the record. Do you any of you have a more updated chart than the one that has been provided today?

Mr. SMITH. No.

Mr. KREBS. No.

Senator ROUNDS. No? No, okay.

For the record, that was done in 2013.

At the same time, for Mr. Krebs, let me just ask. As I understand it, DHS is responsible for the protection of some but not all of the critical infrastructure within the United States. I believe I am correct in my understanding that when it comes to the energy sector, the Department of Energy is the lead agency. Is that correct, sir?

Mr. KREBS. Yes, sir. That is correct.

Senator ROUNDS. Where does it fit in the chart?

Mr. KREBS. So in the column here in the middle, protect critical infrastructure, there is an updated piece of policy surrounding this. I mentioned in my opening statement there is a progressive policy arc. This was a snapshot in time, 2013. The general muscle movements hold and have been reflected in Presidential Policy Directive 41.

Senator ROUNDS. So do you have an updated chart someplace?

Mr. KREBS. I may have something better than a chart. What I have is a plan and a policy around it, PPD 41 and the NCIRP, which lay out the responsibilities of our respective organizations.

Senator ROUNDS. All of you are working on the same level as Mr. Krebs has described here with the information that he has? A yes or a no would be appropriate.

Mr. RAPUANO. Yes, Senator.

Mr. SMITH. Yes.

Senator ROUNDS. Yes. Thank you. I appreciate that because what really would have bothered me is if this thing had not been updated or that you had not been working on anything since 2013 with all the changes that have occurred.

Let me ask just very quickly. I am just curious. It would seem to me that there is no doubt that there are three types of barriers that we need to overcome in order to strengthen the collective cyber defense of the Nation, legal organization and cultural. Have any of you identified legislative hurdles that restrict or prohibit interagency gaps and/or seams for our collective cyber defense? Mr. Rapuano?

Mr. RAPUANO. Senator, I would just note when you look at the National Response Framework that we use for non-cyber but kinetic in the range of state actor or natural events, what you see, particularly since Katrina, is a maturation of a very similar process, many disparate roles, responsibilities, and authorities and many different target stakeholders who may require assistance from local, State, all the way up. This system, the National Cyber Response Framework, is based very closely on that National Response Framework. We are obviously in a more nascent stage when comes to cyber and all the aspects, but I would just say if you look at the last several months in terms of very significant multiple hurricanes and what I think overall, in light of the consequences,

was a very effective federal response, there has been a dramatic evolution in our ability to work as a whole-of-government team when it comes to complex problems with colliding authorities.

Senator ROUNDS. I do have one more question. I get the gist of what you are suggesting.

Let me just ask this in terms of the overall picture here. We can either have defense here within our country, or we can have defense which is to try to stop something in terms of a cyber attack before it actually gets here. That involves not only a cyber system which is universal, it involves talking about systems that are sometimes in our ally's country, sometimes in countries that are not necessarily our friends, but then also in areas where there actually are the bad guys located who are creating the attacks themselves.

What are your views on the sovereignty as it relates to cybersecurity? Let me just add before you answer this.

In Afghanistan, regardless of what you think about the strategy, the longstanding undertone that justifies why we are still there is that fighting the enemy abroad prevents another major attack at home. In this context, it is a defensive strategy played out via offensive maneuvering.

As we evolve cyber and the cyber intelligence fields, it is inevitable that we will start to think of cyber defense in this offensively minded way.

Given this, I would like to hear from you your thoughts on the sovereignty and where we ought to be fighting this battle to stop the attacks before they get here.

Mr. RAPUANO. Senator, that is a very important question. As I think you are aware, the concepts of sovereignty are still molting to some degree in the sense that there are differing views with regard to what constitutes sovereignty in what type of scenario or situation.

Senator ROUNDS. It is, except for one thing. Mr. Chairman, if you would not mind.

Here is the key part of this. These attacks are going on now. Tallin, Tallin 1.0, Tallin 2.0 and so forth are discussions about what our allies are looking at in terms of the sovereignty issues outside. But in the meantime, we have got a gap in time period here in which we have to make a decision about where we actually defend our country against the possibility of existing attacks today, tomorrow, and next week. Now, unless we have got a current strategy with regard to how we regard sovereignty and where we will actually go to defend our critical infrastructure—and I guess that is what I am asking. Do we have that on the books today, and are you prepared to say that we know where we would defend against those attacks? Are we prepared to take them beyond our borders?

Mr. RAPUANO. So, Senator, yes, we do. The details of our current posture with regard to those elements I think would need to be deferred to a closed hearing.

Senator ROUNDS. Very good.

Mr. Smith, Mr. Krebs?

Mr. KREBS. It is a home and away game. We have got to go get them over there at the same time we need to be protecting our infrastructure here. I work very closely, for instance, with the electricity sector in the Electricity Sector Coordinating Council. During

the hurricanes, I was on the phone with the CEOs [Chief Executive Officers] of major utilities on a daily basis. Every 5 p.m. with Secretary Perry, we were talking about the status of the electricity sector. We have to start here, network protection, close out the gaps, mitigate consequences. At the same time, we have to take down the threat actor. It is a whole-of-government best athlete approach.

Senator ROUNDS. Thank you.

Thank you, Mr. Chairman. I apologize for going over, but I think it is a critical issue that we have to address. Thank you.

Chairman MCCAIN. Senator Rounds, thank you for what you and Senator Nelson have been doing.

Senator Blumenthal?

Senator BLUMENTHAL. Thanks, Mr. Chairman. Thank you very much for holding this critically important hearing and to the excellent witnesses that we have before us today.

This week, the "New York Times" published an article—and I am going to submit it for the record, assuming there is no objection—which details North Korea's cyber attacks that are estimated to provide the North Korean Government with as much as $1 billion a year.

[The information follows:]

The New York Times | https://nyti.ms/2zbZfd4

ASIA PACIFIC

The World Once Laughed at North Korean Cyberpower. No More.

查看简体中文版
查看繁體中文版

By DAVID E. SANGER, DAVID D. KIRKPATRICK and NICOLE PERLROTH OCT. 15, 2017

When North Korean hackers tried to steal $1 billion from the New York Federal Reserve last year, only a spelling error stopped them. They were digitally looting an account of the Bangladesh Central Bank, when bankers grew suspicious about a withdrawal request that had misspelled "foundation" as "fandation."

Even so, Kim Jong-un's minions still got away with $81 million in that heist.

Then only sheer luck enabled a 22-year-old British hacker to defuse the biggest North Korean cyberattack to date, a ransomware attack last May that failed to generate much cash but brought down hundreds of thousands of computers across dozens of countries — and briefly crippled Britain's National Health Service.

Their track record is mixed, but North Korea's army of more than 6,000 hackers is undeniably persistent, and undeniably improving, according to American and British security officials who have traced these attacks and others back to the North.

Amid all the attention on Pyongyang's progress in developing a nuclear weapon capable of striking the continental United States, the North Koreans have also

quietly developed a cyberprogram that is stealing hundreds of millions of dollars and proving capable of unleashing global havoc.

Unlike its weapons tests, which have led to international sanctions, the North's cyberstrikes have faced almost no pushback or punishment, even as the regime is already using its hacking capabilities for actual attacks against its adversaries in the West.

And just as Western analysts once scoffed at the potential of the North's nuclear program, so did experts dismiss its cyberpotential — only to now acknowledge that hacking is an almost perfect weapon for a Pyongyang that is isolated and has little to lose.

The country's primitive infrastructure is far less vulnerable to cyberretaliation, and North Korean hackers operate outside the country, anyway. Sanctions offer no useful response, since a raft of sanctions are already imposed. And Mr. Kim's advisers are betting that no one will respond to a cyberattack with a military attack, for fear of a catastrophic escalation between North and South Korea.

"Cyber is a tailor-made instrument of power for them," said Chris Inglis, a former deputy director of the National Security Agency, who now teaches about security at the United States Naval Academy. "There's a low cost of entry, it's largely asymmetrical, there's some degree of anonymity and stealth in its use. It can hold large swaths of nation state infrastructure and private-sector infrastructure at risk. It's a source of income."

Mr. Inglis, speaking at the Cambridge Cyber Summit this month, added: "You could argue that they have one of the most successful cyberprograms on the planet, not because it's technically sophisticated, but because it has achieved all of their aims at very low cost."

It is hardly a one-way conflict: By some measures the United States and North Korea have been engaged in an active cyberconflict for years.

Both the United States and South Korea have also placed digital "implants" in the Reconnaissance General Bureau, the North Korean equivalent of the Central

Intelligence Agency, according to documents that Edward J. Snowden released several years ago. American-created cyber- and electronic warfare weapons were deployed to disable North Korean missiles, an attack that was, at best, only partially successful.

Indeed, both sides see cyber as the way to gain tactical advantage in their nuclear and missile standoff.

A South Korean lawmaker last week revealed that the North had successfully broken into the South's military networks to steal war plans, including for the "decapitation" of the North Korean leadership in the opening hours of a new Korean war.

There is evidence Pyongyang has planted so-called digital sleeper cells in the South's critical infrastructure, and its Defense Ministry, that could be activated to paralyze power supplies and military command and control networks.

But the North is not motivated solely by politics: Its most famous cyberattack came in 2014, against Sony Pictures Entertainment, in a largely successful effort to block the release of a movie that satirized Mr. Kim.

What has not been disclosed, until now, is that North Korea had also hacked into a British television network a few weeks earlier to stop it from broadcasting a drama about a nuclear scientist kidnapped in Pyongyang.

Once North Korea counterfeited crude $100 bills to try to generate hard cash. Now intelligence officials estimate that North Korea reaps hundreds of millions of dollars a year from ransomware, digital bank heists, online video game cracking, and more recently, hacks of South Korean Bitcoin exchanges.

One former British intelligence chief estimates the take from its cyberheists may bring the North as much as $1 billion a year, or a third of the value of the nation's exports.

The North Korean cyberthreat "crept up on us," said Robert Hannigan, the former director of Britain's Government Communications Headquarters, which handles electronic surveillance and cybersecurity.

"Because they are such a mix of the weird and absurd and medieval and highly sophisticated, people didn't take it seriously," he said. "How can such an isolated, backward country have this capability? Well, how can such an isolated backward country have this nuclear ability?"

From Minor Leaguers to Serious Hackers

Kim Jong-il, the father of the current dictator and the initiator of North Korea's cyberoperations, was a movie lover who became an internet enthusiast, a luxury reserved for the country's elite. When Mr. Kim died in 2011, the country was estimated to have 1,024 IP addresses, fewer than on most New York City blocks.

Mr. Kim, like the Chinese, initially saw the internet as a threat to his regime's ironclad control over information. But his attitude began to change in the early 1990s, after a group of North Korean computer scientists returned from travel abroad proposing to use the web to spy on and attack enemies like the United States and South Korea, according to defectors.

North Korea began identifying promising students at an early age for special training, sending many to China's top computer science programs. In the late 1990s, the Federal Bureau of Investigation's counterintelligence division noticed that North Koreans assigned to work at the United Nations were also quietly enrolling in university computer programming courses in New York.

"The F.B.I. called me and said, 'What should we do?' " recalled James A. Lewis, at the time in charge of cybersecurity at the Commerce Department. "I told them, 'Don't do anything. Follow them and see what they are up to.'"

The North's cyberwarfare unit gained priority after the 2003 invasion of Iraq by the United States. After watching the American "shock and awe" campaign on CNN, Kim Jong-il issued a warning to his military: "If warfare was about bullets and oil until now," he told top commanders, according to a prominent defector, Kim Heung-kwang, "warfare in the 21st century is about information."

The unit was marked initially by mishaps and bluster.

"There was an enormous growth in capability from 2009 or so, when they were a joke," said Ben Buchanan, the author of "The Cybersecurity Dilemma" and a fellow at the Cyber Security Project at Harvard. "They would execute a very basic attack against a minor web page put up by the White House or an American intelligence agency, and then their sympathizers would claim they'd hacked the U.S. government. But since then, their hackers have gotten a lot better."

A National Intelligence Estimate in 2009 wrote off the North's hacking prowess, much as it underestimated its long-range missile program. It would be years before it could mount a meaningful threat, it claimed.

But the regime was building that threat.

When Kim Jong-un succeeded his father, in 2011, he expanded the cybermission beyond serving as just a weapon of war, focusing also on theft, harassment and political-score settling.

"Cyberwarfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike relentlessly," Kim Jong-un reportedly declared, according to the testimony of a South Korean intelligence chief.

And the array of United Nations sanctions against Pyongyang only incentivized Mr. Kim's embrace.

"We're already sanctioning anything and everything we can," said Robert P. Silvers, the former assistant secretary for cyberpolicy at the Department of Homeland Security during the Obama administration. "They're already the most isolated nation in the world."

By 2012, government officials and private researchers say North Korea had dispersed its hacking teams abroad, relying principally on China's internet infrastructure. This allowed the North to exploit largely nonsecure internet connections and maintain a degree of plausible deniability.

A recent analysis by the cybersecurity firm Recorded Future found heavy North Korean internet activity in India, Malaysia, New Zealand, Nepal, Kenya, Mozambique, and Indonesia. In some cases, like that of New Zealand, North Korean

hackers were simply routing their attacks through the country's computers from abroad. In others, researchers believe they are now physically stationed in countries like India, where nearly one-fifth of Pyongyang's cyberattacks now originate.

Intelligence agencies are now trying to track the North Korean hackers in these countries the way they have previously tracked terrorist sleeper cells or nuclear proliferators: looking for their favorite hotels, lurking in online forums they may inhabit, attempting to feed them bad computer code and counterattacking their own servers.

Learning From Iran, Growing Bolder

For decades Iran and North Korea have shared missile technology, and American intelligence agencies have long sought evidence of secret cooperation in the nuclear arena. In cyber, the Iranians taught the North Koreans something important: When confronting an enemy that has internet-connected banks, trading systems, oil and water pipelines, dams, hospitals, and entire cities, the opportunities to wreak havoc are endless.

By midsummer 2012, Iran's hackers, still recovering from an American and Israeli-led cyberattack on Iran's nuclear enrichment operations, found an easy target in Saudi Aramco, Saudi Arabia's state-owned oil company and the world's most valuable company.

That August, Iranian hackers flipped a kill switch at precisely 11:08 a.m., unleashing a simple wiper virus onto 30,000 Aramco computers and 10,000 servers that would destroy data, and replace it with a partial image of a burning American flag. The damage was tremendous.

Seven months later, during joint military exercises between American and South Korean forces, North Korean hackers, operating from computers inside China, deployed a very similar cyberweapon against computer networks at three major South Korean banks and South Korea's two largest broadcasters. Like Iran's Aramco attacks, the North Korean attacks on South Korean targets used wiping malware to eradicate data and paralyze their business operations.

It may have been a copycat operation, but Mr. Hannigan, the former British official, said recently: "We have to assume they are getting help from the Iranians."

And inside the National Security Agency, just a few years after analysts had written off Pyongyang as a low grade threat, there was suddenly a new appreciation that the country was figuring out cyber just as it had figured out nuclear weapons: test by test.

"North Korea showed that to achieve its political objectives, it will take down any company — period," Mr. Silvers said.

Protecting Kim's Image

A chief political objective of the cyberprogram is to preserve the image of the North's 33-year-old leader, Kim Jong-un. In August 2014, North Korean hackers went after a British broadcaster, Channel Four, which had announced plans for a television series about a British nuclear scientist kidnapped in Pyongyang.

First, the North Koreans protested to the British government. "A scandalous farce," North Korea called the series. When that was ignored, British authorities found that the North had hacked into the television network's computer system. The attack was stopped before inflicting any damage, and David Abraham, the chief executive of Channel Four, initially vowed to continue the production.

That attack, however, was just a prelude. When Sony Pictures Entertainment released a trailer for "The Interview," a comedy about two journalists dispatched to Pyongyang to assassinate North Korea's young new dictator, Pyongyang wrote a letter of complaint to the secretary general of the United Nations to stop the production. Then came threats to Sony.

Michael Lynton, then Sony's chief executive, said when Sony officials called the State Department, they were told it was just more "bluster," he said.

"At that point in time, Kim Jong-un was relatively new in the job, and I don't think it was clear yet how he was different from his father," Mr. Lynton said in an interview. "Nobody ever mentioned anything about their cyber capabilities."

In September 2014, while still attempting to crack Channel 4, North Korean hackers buried deep into Sony's networks, lurking patiently for the next three months, as both Sony and American intelligence completely missed their presence.

The director of national intelligence, James Clapper, was even in Pyongyang at the time, trying to win the release of a detained American, and had dinner with the then-chief of the Reconnaissance General Bureau.

On Nov. 24, the attack on Sony began: Employees arriving at work that day found their computer screens taken over by a picture of a red skeleton with a message signed "GOP," for "Guardians of Peace."

"We've obtained all your internal data including your secrets and top secrets," the message said. "If you don't obey us, we'll release data shown below to the world."

That was actually a diversion: The code destroyed 70 percent of Sony Pictures' laptops and computers. Sony employees were reduced to communicating via pen, paper and phone.

Mr. Lynton said the F.B.I. told him that nothing could have been done to prevent the attack, since it was waged by a sovereign state. "We learned that you really have no way of protecting yourself in any meaningful way," he said of such nation-state attacks.

Sony struggled to distribute the film as theaters were intimidated. (Ultimately it was distributed for download, and may have done better than it would have.) In London, outside investors in Channel Four's North Korea project suddenly dried up, and the project effectively died.

The Obama White House responded to the Sony hack with sanctions that the North barely noticed, but with no other retaliation. "A cyberbattle would be a lot more risky for the United States and its allies than for North Korea," said Mr. Silvers.

Robbing Banks, Pyongyang Style

Beyond respect, and retribution, the North wanted hard currency from its cyberprogram.

So soon the digital bank heists began — an attack in the Philippines in October 2015; then the Tien Phong Bank in Vietnam at the end of the same year; and then the Bangladesh Central Bank. Researchers at Symantec said it was the first time a state had used a cyberattack not for espionage or war, but to finance the country's operations.

Now, the attacks are increasingly cunning. Security experts noticed in February that the website of Poland's financial regulator was unintentionally infecting visitors with malware.

It turned out that visitors to the Polish regulator's website — employees from Polish banks, from the central banks of Brazil, Chile, Estonia, Mexico, Venezuela, and even from prominent Western banks like Bank of America — had been targeted with a so-called watering hole attack, in which North Korean hackers waited for their victims to visit the site, then installed malware in their machines. Forensics showed that the hackers had put together a list of internet addresses from 103 organizations, most of them banks, and designed their malware to specifically infect visitors from those banks, in what researchers said appeared to be an effort to move around stolen currency.

More recently, North Koreans seemed to have changed tack once again. North Korean hackers' fingerprints showed up in a series of attempted attacks on so-called cryptocurrency exchanges in South Korea, and were successful in at least one case, according to researchers at FireEye.

The attacks on Bitcoin exchanges, which see hundreds of millions of dollars worth of Bitcoin exchanged a day, offered Pyongyang a potentially very lucrative source of new funds. And, researchers say, there is evidence they have been exchanging Bitcoin gathered from their heists for Monero, a highly anonymous version of cryptocurrency that is far harder for global authorities to trace.

The most widespread hack was WannaCry, a global ransomware attack that used a program that cripples a computer and demands a ransom payment in exchange for unlocking the computer, or its data. In a twist the North Koreans surely enjoyed, their hackers based the attack on a secret tool, called "Eternal Blue," stolen from the National Security Agency.

In the late afternoon of May 12, panicked phone calls flooded in from around Britain and the world. The computer systems of several major British hospital systems were shut down, forcing diversions of ambulances and the deferral of nonemergency surgeries. Banks and transportation systems across dozens of countries were affected.

Britain's National Cyber Security Center had picked up no warning of the attack, said Paul Chichester, its director of operations. Investigators now think the WannaCry attack may have been an early misfire of a weapon that was still under development — or a test of tactics and vulnerabilities.

"This was part of an evolving effort to find ways to disable key industries," said Brian Lord, a former deputy director for intelligence and cyber operations at the Government Communications Headquarters in Britain. "All I have to do is create a moderately disabling attack on a key part of the social infrastructure, and then watch the media sensationalize it and panic the public."

It ended thanks to Marcus Hutchins, a college dropout and self-taught hacker living with his parents in the southwest of England. He spotted a web address somewhere in the software and, on a lark, paid $10.69 to register it as a domain name. The activation of the domain name turned out to act as a kill switch causing the malware to stop spreading.

British officials privately acknowledge that they know North Korea perpetrated the attack, but the government has taken no retaliatory action, uncertain what they can do.

A Cyber Arms Race

While American and South Korean officials often express outrage about North Korea's cyberactivities, they rarely talk about their own — and whether that helps fuel the cyber arms race.

Yet both Seoul and Washington target the North's Reconnaissance General Bureau, its nuclear program and its missile program. Hundreds, if not thousands, of

American cyberwarriors spend each day mapping the North's few networks, looking for vulnerabilities that could be activated in time of crisis.

At a recent meeting of American strategists to evaluate North Korea's capabilities, some participants expressed concerns that the escalating cyberwar could actually tempt the North to use its weapons — both nuclear and cyber — very quickly in any conflict, for fear that the United States has secret ways to shut the country down.

The director of the Central Intelligence Agency, Mike Pompeo, said last week that the United States is trying to compile a better picture of the leadership around Kim Jong-un, for a report to President Trump. Figuring out who oversees cyber and special operations is a central mystery. The Japanese press recently speculated it could be an official named Jang Kil-su. Others are curious about Gen. No Kwang-chol, who was elevated to the Central Committee of the North's ruling party in May 2016, and is one of the only members whose portfolio is undisclosed.

The big question is whether Mr. Kim, fearful that his nuclear program is becoming too large and obvious a target, is focusing instead on how to shut down the United States without ever lighting off a missile. "Everyone is focused on mushroom clouds," Mr. Silvers said, "but there is far more potential for another kind of disastrous escalation."

Choe Sang-Hun contributed reporting from Seoul.

A version of this article appears in print on October 16, 2017, on Page A1 of the New York edition with the headline: North Korea Deploys Corps Of Hackers Bent on Chaos.

© 2017 The New York Times Company

Senator BLUMENTHAL. That figure is staggering. It is equivalent to one-third of that country's total exports. North Korea's ransomware attacks and cyber attacks on banks around the world are producing a funding stream for that country, which in turn fuels its nuclear program. It is a funding source that must be stopped. At a time when the United States is leading efforts to sanction exports of coal, labor, textiles, and other products, in order to hinder North Korea's nuclear ambitions, we also have to be focusing on additional funding sources. This cash flow ought to be priority number one. Tough rhetoric must be supported by tough action and practical measures that make clear to North Korea that this kind of conduct will be answered.

So the question is what actions are being taken to combat their offensive cyber operations and address this cyber revenue. I know that you may not be fully at liberty to discuss these steps in this forum, but I would like you to do so to the extent you can because North Korea knows what it is doing. You are not going to reveal anything to North Korea. The American people deserve to know what North Korea is doing and they do not. So this is a topic that I think ought to be front and center for the administration and for the Congress and for the American people. I look forward to your responses.

Mr. RAPUANO. I would simply say, yes, Senator, we do have plans and capabilities that are focused and directed on the North Korean threat in general and on the specific activities that you have noted. I think that it would be most appropriate, if we are going into detail, to do that in closed session.

Mr. SMITH. Senator, I would just say that we continue to work with our foreign partners in information sharing whenever possible when we are able to assist them in identifying these types of criminal activities. We provide them also technical assistance whenever asked or engaging with them in joint operations. Whenever possible, we are always looking to link it back or coordinate some indictment or investigative—some joint operation that would bring to light the people or the nation states that are conducting those activities.

Mr. KREBS. I will pile on here and actually provide a little bit of detail on a particular unclassified activity. Working very closely with the FBI, we designated one effort called Hidden Cobra. On US–CERT [U.S.-Computer Emergency Readiness Team], we have a Hidden Cobra page that speaks to a botnet infrastructure, command and control infrastructure, that has certain indicators, that, hey, look at this. Go track this down. Working with federal partners where some of that command and control infrastructure may be in another country, we share that information with them, and we are looking to take action against it. So this is not just a whole-of-government approach, this is an international problem with international solutions. We are moving out aggressively. This is recent, last few weeks, where we have been able to partner some unlikely partners.

Senator BLUMENTHAL. I agree that it is an international problem with international solutions. But we provide the main solution, and we are, in effect, victims substantially if not primarily of the problem. I understand, Mr. Rapuano, that we have plans and capabili-

ties. I am not fully satisfied with the idea that those forward-oriented measures of action are sufficient. I think we need action here and now.

The Lazarus Group, a North Korean-linked cyber crime ring, stole $81 million from the Bangladesh Central Bank account at the New York Federal Reserve, which would have been $1 billion but for a spelling error, a fairly rudimentary spelling error on the part of North Koreans. They have also been tied to the WannaCry attack earlier this year and the Sony attack in 2014. This week they are being linked to a $60 million theft from the Taiwanese Bank. Measured in millions, given the way we measure amounts of money and this week with our budget in the billions and trillions, this may seem small but it is substantial given the North Korean economy and its size. So I am hoping that in another setting we can be more fully briefed on what is being done now to stem and stop this threat.

I appreciate all of your good work in this area. Thank you.

Thanks, Mr. Chairman.

Chairman MCCAIN. Senator Ernst?

Senator ERNST. Thank you, gentlemen, for your willingness to tackle these issues. I think it goes without saying that your level of success in these areas will really influence American democracy for many, many years, as well as decades to come.

So the conversation today so far has been focused very much on cyber defense coordination, which we would all say is very important. However, coordination does not do any good without the proper understanding of our capabilities across the Government. That is why I worked with Senators Coons, Fischer, and Gillibrand to introduce bipartisan legislation requiring the DOD to track National Guard cyber capabilities. Mr. Smith, you had given a shoutout to the new cyber program within the National Guard, and I really do appreciate that.

So for each of you, how do you assess the capabilities of the individuals and the organizations under your charge? Because we see this lovely chart which is very old. But you do have a number of organizations that you are responsible for. How do you go in and assess what that organization can actually do and is it effective? So it is great to say, hey, we have a cyber team in DOJ or whatever, but how do you know that they are effective? Can you explain how you assess that? We will start with you, Mr. Secretary.

Mr. RAPUANO. Thank you, Senator. That is an excellent question and it does represent a significant challenge. We have got a lot of disparate organizations that obviously have cyber equities and are developing cyber capabilities. Within the Department of Defense, we have really committed in earnest to start to better understand the cross-cut in terms of the services, the commands, the full range, including the National Guard, what are their capabilities, what specific skills are they developing, what professional development program do we have to recruit, train, and develop very attractive career paths for the best and the brightest.

So we have a number of initiatives, starting with the budget initiative. So when you start to see our budget formulations, it is apples to apples instead of what it has been historically which is each service's or organization's conception of what constitutes training or

what constitutes the different elements of their budget. We did a first run this year that was off the budget cycle just to get us in the road to progress, so to speak, and we found that we really have got to ensure that there is common definitional issues so we were defining things the same way.

The other area, in terms of the National Guard, we do track National Guard cyber capability development, training capabilities, and how they fit into the Cyber Mission Force. The one area that we do have a little bit of a challenge with is under State status, we do not have that same system of consistent definitions. So that is something that we are working at, but we definitely recognize the critical importance of having that common ability of across many different fronts to define those things so we can apply them——

Senator ERNST. No. I appreciate that. That is good to understand that now and get those worked out—those details and discrepancies worked out.

Mr. Smith, how about you?

Mr. SMITH. On our technical side, we tend to be on the job with that routinely. So most of the people who are out are currently actively engaged in either incidents response and following up on the threats and investigations. But we spend a significant amount of effort in enhancing those particularly at a much higher level on the cyber technical side.

But in addition to that, we have taken steps to significantly elevate the entire workforce in the digital domain. We have created on-the-job training which allows non-cyber personnel to be taken offline from investigating other matters to enhance that cyber capability so when they go back after a couple of months, they are capable of bringing both their normal traditional investigative methods along with the current modern digital investigative requirements.

Looking longer term, though, when we are talking about the workforce of the future, we have been collaborating on a much more local level with STEM [Science, Technology, Engineering and Mathematics] high schools programs in developing and building a future workforce as opposed to trying to compete with everybody here and with the private industry, which can offer things and more benefits at times than we are capable of, but by building in FBI cyber STEM programs and bringing local university courses to high school students at an earlier age and supplementing that with some leadership development in those high school ranks. So looking long term building a workforce that will augment and maintain the necessity that we all require we are talking about here in this digital arena. Working with the non-cyber elements, our internal cyber people—they are at a very high level.

Senator ERNST. Yes. I am running out of time. Mr. Krebs, if you could submit that to us for the record, I would be appreciative.

[The information follows:]

At the National Protection and Programs Directorate (NPPD), we have thousands of employees located throughout the Nation who are well qualified to carry out our mission. We assess the capabilities of these employees through our rigorous hiring process and continue assessing their capabilities through annual performance reviews. We also invest in training and professional development opportunities to ensure our employees remain at the forefront of the mission.

There is often no single solution to security practices, and innovation, critical thinking, and diversity of opinion increase our likelihood for success. Accountability is critical to ensuring success as a team; success is rewarded, and falling short of goals presents opportunities to improve and correct. By communicating expectations and roles to team members, empowering them, and ensuring they have resources enables them and our organization to be successful. It is important to focus on putting the right people in the right jobs with the right responsibilities.

Measuring success for any homeland security enterprise is challenging because typically success means we have prevented something from happening. For NPPD, success means we are receiving and sharing information in a timely manner, deploying resources where requested by our stakeholders, and providing actionable security recommendations which will raise the overall level of security across the nation. However, recognizing that perfect security is virtually impossible, we will continue moving towards an "assume breach" posture, ensuring that we are prepared to minimize the damage an attacker can inflict. Useful metrics in this vein are (1) time to detection of the adversary, (2) time to investigate the attack, and (3) time to mitigate the damage and evict the adversary. Our goal should be to get these time values to hours if not minutes, where they may now be weeks or even months.

NPPD also tracks trends that provide insight into our overall level of security and the usefulness of the products and services we offer, such as rate of compliance with the Department of Homeland Security's Binding Operational Directive mandates, our ability to implement cybersecurity hygiene practices, and use of DHS services and capabilities by our stakeholders.

Senator ERNST. But, gentlemen, one thing too, as we look across the board, is really assessing those organizations that fall under your purview but then making sure that we are not duplicating services amongst our agencies as well and operating as efficiently as possible. So thank you very much.

Thank you, Mr. Chair.

Chairman MCCAIN. Senator Hirono?

Senator HIRONO. Thank you, Mr. Chairman.

I am glad that we are having a discussion about the integrity of our elections as being fundamental to our democracy.

Mr. Krebs, as I look at this chart, even if it is dated, your responsibility at DHS is to protect critical infrastructure, and you did say that election systems are critical infrastructure. You have an election security task force. So do you consider DHS to be the lead agency on making sure that our election systems are not hacked?

Mr. KREBS. Ma'am, we need statutory authorities to coordinate protection activities across the critical infrastructure, and as a designated critical infrastructure subsector, yes, ma'am, I lead in coordinating.

Now, I do not physically protect those networks. I enable State and locals and also the private sector to have better practices. Yes, ma'am.

Senator HIRONO. I understand that, but you would be the lead federal agency that would have this responsibility to work with the State and local entities to protect our election systems.

Mr. KREBS. From a critical infrastructure protection perspective, yes, ma'am, alongside the FBI, as well as the intelligence community.

Senator HIRONO. What we are just looking for, as we are wrestling with the idea of who is responsible for what, I would just like to get down that with regard to election systems, we should look to DHS. That is all I want to know.

Now, I hope that your task force is also addressing the purchases of political ads by foreign countries. I hope that is one of the things

that your task force will address and whether there is a need for legislation to prevent those kind of purchases.

I want to get to a question to Mr. Rapuano. Data protection is obviously an important issue with industrial espionage being carried out by some of our near-peer competitors. The DOD requires contractors to provide adequate security for our covered defense information that is processed, stored, or transmitted on the contractor's internal information system or network. By December 31st, 2017, contractors must, at a minimum, implement security requirements to meet the National Institute of Standards and Technology NIST, standards.

So my question, Mr. Rapuano, can you talk about the importance of having industry comply with this requirement and how you are working with industry to get the word out so that everyone is aware, especially I would say small businesses that you all work with? They need to know that they are supposed to be doing this.

Mr. RAPUANO. Yes, Senator. Our primary focus is with the defense industrial base where we have the highest frequency and most significant DOD programs. But we are engaged with all of those private sector elements that work with the Department of Defense. I work that closely with the Chief Information Officer for the Department, Dr. Zangardi. I can get you additional details on the processes for doing that.

Senator HIRONO. Yes. I would like to make sure that, as I mentioned, particularly small businesses who may not be aware of this requirement, that they are very aware and that they have enough time to comply because December 2017 is just right around the corner. So whatever you have, fliers, whatever you use to get the word out.

Mr. Rapuano did not respond in time for printing. When received, answer will be retained in committee files.

Senator HIRONO. For Mr. Krebs, you mentioned in your testimony how cyber actors have strategically targeted critical infrastructure sectors with the intent ranging from cyber espionage to disruption of critical services. Specifically you identified two malware attacks called BlackEnergy and Havoc. Is that the right pronunciation?

Mr. KREBS. Yes, ma'am.

Senator HIRONO. They have specifically targeted industrial control systems. It does not take a lot of imagination to think of how a sophisticated cyber attack to a power plant's industrial control system could cause a massive disruption with grave consequences.

What is being done by DHS to encourage the private sector to harden their defense of industrial control systems?

Mr. KREBS. Yes, ma'am. Thank you for your question, and I do share your concern particularly with respect to those two toolkits.

I think I would answer the question two ways. One, an endpoint protection. So we do work very closely with the electricity sector, as I mentioned early on, with the Electricity Sector Coordinating Council, again from a grid perspective. But then through our industrial control systems CERT, the ICS–CERT, we do look at kind of more scalable solutions that I mentioned in my opening statement, not just kind of the whack-a-mole approach at the individual facilities but try to understand what the actual individual control sys-

tems are, who manufactures them because it does tend to be a smaller set of companies. Instead of 100 or 1,000 endpoints, we can kind of go to the root of the problem, the systemic problem, as I also mentioned, address that at the manufacturer or coder level and then from there, kind of break out and hit those endpoints. So again, we do work at the endpoint, but we also work at kind of the root problem.

Senator HIRONO. So you perform outreach activities then through ICS–CERT to make sure that, for example, the utility sector is adequately——

Mr. KREBS. Among other mechanisms, yes, ma'am.

Senator HIRONO. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Tillis?

Senator TILLIS. Thank you, Mr. Chairman.

Gentlemen, thank you for being here.

One quick question, and this is really from my perspective as the Personnel Subcommittee chair. What trends, either positive or negative, are we seeing? Mr. Rapuano, you mentioned I think earlier when I was here about the National Guard playing some role at the State level. But can you give me any idea, either positive or concerning trends, about the resources we are getting into the various agencies to really flesh out our expertise to attract them and retain them and to grow them?

Mr. RAPUANO. Well, I would simply say—and I think it has been a common experience for my colleagues at the table here—that getting the best talent is a very significant challenge in the cyber realm for all the obvious reasons.

Senator TILLIS. Compensation? I mean, there is a variety of reasons, but what would you list as the top two or three?

Mr. RAPUANO. There is a very high demand signal throughout the entire economy. The compensation that individuals can get on the outside of government is significantly greater. We are trying to address that in terms of our workforce management process, and we have some additional authorities that we are applying to that, as I believe other agencies have as well. But, again, it is a demand versus supply question.

Senator TILLIS. We have had this discussed before, and actually Senator Rounds and I have talked about it. I would be very interested in feedback that you can give us on things that we should look at as a possible subject matter for future subcommittee hearings for retention. I worked in the private sector, and I had a cyber subpractice, ethical hack testing practice, back in the private sector. What you are up against is not only a higher baseline for salaries, but you are also up against what the industry would call hot skills. These are very, very important skills. Just when you think you have caught up or got within the range on the baseline comp, a firm, like the firm that I worked with, both Price Waterhouse and IBM [International Business Machines] says, okay, now we have got to come in with a signing bonus and some sort of retention measures that make it impossible in a governmental institution to stay up with. So getting feedback on that would be helpful.

I am going to be brief because we have got votes and I want to stick to my time.

I do want to just associate myself with the comments and questions that were made by Senator Inhofe and I think Senator Shaheen about open source software and some of the policy discussions we are having here. I will go back to the record to see how you all responded to their questions, but I share their concern.

I want to get more of an idea of the scope and the scale of non-classified software that the Department uses. I am trying to get an idea of a volume, let us say, as a percentage of the entire portfolio. What are we looking at at non-classified software as a percentage of our base? I mean, is it safe to assume that it is in the thousands in terms of platforms, tools, the whole portfolio of the technology stack?

Mr. RAPUANO. Senator, that is a request that I have in to our system and to our CIO's office, and I can get that information back to you as soon as I get it.

Mr. SMITH. Yes. I would have to get back with you with more specifics.

Senator TILLIS. I think it would be helpful because I am sure that we have application portfolios out there—I hope, I should say—that we are following best practices. Somebody out there in the ops world knows exactly what our portfolio is and how they fit in the classified and unclassified realm. I think that would be very helpful, very instructive to this committee.

I am going to yield back the rest of my time so hopefully other members can get their questions in before the vote. Thank you, Mr. Chair.

Chairman MCCAIN. Senator King?

Senator KING. Mr. Krebs, I just want to make you feel better about your title. I enjoyed that interplay with Senator Shaheen. 40 years ago I worked here as a staff member, and I was seeking a witness—I think I may have told the chairman this story—from the Office of Management and Budget from the administration. They said he is the Deputy Secretary under such and such. I said I do not know what that title means. The response was—and you can take this home with you—he is at the highest level where they still know anything. I now realize, by the way, that I am above that level. But I appreciate having you here.

I think you fellows understated one important point, and I do not understand why the representative from the White House is not here because I think he has a reasonable story to tell. On May 11th, the President issued a pretty comprehensive executive order on this subject that is not the be-all and end-all on the subject, but certainly is an important beginning.

Now, here is my question, though. In that executive order, there were a number of report-back requirements that triggered mostly in August. My question is have those report-backs been done. Mr. Rapuano?

Mr. RAPUANO. Senator, they are starting to come in. As you note, there are a number that are still due out.

Senator KING. Some were 180 days, some were 90 days. So I am wondering if the 90 days, which expired in August, have come back.

Mr. RAPUANO. That is correct. I do not have the full tracker with me right here. I can get back to you on that.

Senator KING. I would appreciate that.

[The information follows:]

Mr. Rapuano did not respond in time for printing. When received, answer will be retained in committee files.

Mr. RAPUANO. Some have been submitted according to the original timeline. Others have been extended. But absolutely, those are the essential elements of information necessary to fully develop and update the strategy to the evolving threats and build that doctrine and requirements and plans.

Senator KING. You used the keyword of "doctrine" and I want to talk about that in a minute. But by the same token, this committee passed or the Congress passed as part of the National Defense Authorization Act last December a provision requiring a report from the Secretary of Defense to the President within 180 days and from the President to the Congress within 180 days. That report would have been due in June from the Secretary of Defense involving what are the military and non-military options available for deterring and responding to imminent threats in cyberspace. Do you know if that report has been completed?

Mr. RAPUANO. Yes, Senator. It was our original intent and desire to couple the two with the input both into the President's EO [Executive Order], as well as the input back to the Senate. Based on the delay of the President's EO, we decoupled that because we recognize your impatience and we need to——

Senator KING. You may have picked up some impatience this morning. Do we have it?

Mr. RAPUANO. So we will be submitting it to you shortly, and I will get a specific date for that.

Senator KING. "Shortly" does not make me feel much better. Is that geologic time or is that——

Mr. RAPUANO. Calendar time, Senator.

Senator KING. Please let us know.

You mentioned the word "doctrine," and I think that is one of the key issues here. If all we do is try to patch networks and defend ourselves, we will ultimately lose. Mr. Smith, you used the term "impose consequences." Right now, we are not imposing much in the way of consequences. For the election hacking, which is one of the most egregious attacks on the United States in recent years, there were sanctions passed by the Congress, but it was 6 or 8 months later and it is unclear how severe they will be.

We need a doctrine where our adversaries know if they do X, Y will happen to them. Mr. Rapuano, do you have any thoughts on that? Do you see what I mean? Just being on the defensive is not going to work in the end. If you are in a boxing match and you can bob and weave and you are the best bobber and weaver in the history of the world, if you are not allowed to ever punch, you are going to lose that boxing match.

Mr. RAPUANO. Yes, Senator. I certainly agree that both the demonstrated will and ability to respond to provocations in general and cyber in specific is critical to effective deterrence. I think the challenge that we have that is somewhat unique in cyber is defining a threshold that then does not invite adversaries to inch up close but short of it. Therefore, the criteria—it is very difficult to make

them highly specific versus more general, and then the down side of the general is it is too ambiguous to be meaningful as——

Senator KING. Part of the problem also is we tend to want to keep secret what we can do when, in reality, a secret deterrent is not a deterrent. The other side has to know what is liable to happen to them. I hope you will bear that in mind. I think this is a critically important area because we have to have a deterrent capability. We know this is coming, and so far there has not been much in the way of price paid, whether it was Sony or Anthem-Blue Cross or the Government personnel office or our elections. There have to be consequences, otherwise everybody is going to come after us, not just Russia, but North Korea, Iran, and terrorist organizations. This is warfare on the cheap, and we have to be able not only to defend ourselves but to defend ourselves through a deterrent policy. I hope in the counsels of the administration that will be an emphasis in your response.

Mr. RAPUANO. Yes, I agree, Senator. That is the point of the EO in terms of that deterrence option set is to understand them in the wider context of our capabilities, different authorities, and to start being more definitive about what those deterrence options are and how we can best use them.

Senator KING. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Heinrich?

Senator HEINRICH. I want to return to that because I keep hearing the words, but I do not see something specific in place. We have struggled with this for years on this committee now. Imagine that tomorrow we had a foreign nation state cyber attack on our financial or our banking sector or next month on our utility or our transmission infrastructure or next year on our elections. I would suggest that any of those would cross a threshold. What is our doctrine for how, when, and with what level of proportionality we are going to respond to that kind of a cyber attack? Mr. Rapuano?

Mr. RAPUANO. First, I would note that obviously our deterrence options are expansive beyond cyber per se. So cyber is one of a large number of tools, including diplomatic, economic, trade, military options, kinetic, and then cyber. So looking at that broad space——

Senator HEINRICH. I agree wholeheartedly. You should not limit yourself to responding in kind with the same level of—or with the same toolbox. But do we have a doctrine? Because if we do not have a doctrine—one of the things that worked through the entire Cold War is we knew what the doctrine for the other side was and they knew what our doctrine was. That kept us from engaging in conflicts that neither side wanted to engage in. Do we have an overall structure for how we are going to respond? If we do not, I would suggest we have no way to achieve deterrence.

Mr. RAPUANO. We do not have sufficient depth and breadth of the doctrine as we have been discussing. That really is one of the primary drivers of the executive order, the 13800, is to have the essential elements to best inform that doctrine.

Senator HEINRICH. I mean, the chairman has been asking for an overall plan for I do not know how long. I think that is what we

are all going to be waiting for. I wish I could ask the same question of Mr. Joyce, but maybe in a future hearing.

For any of you, I spent a good part of yesterday looking at Russian-created, Russian-paid for Facebook ads that ran in my State and in places across this country and were clearly designed to divide this country, as well as to have an impact on our elections. What is the administration doing to make sure that in 2018 we are not going to see the same thing all over again? Do not all speak at once.

Mr. KREBS. Sir, yes, let me start with the election infrastructure subsector that we have established. So from a pure cyber attack perspective, we are working with State and local officials to up their level of defense. But specific to the ad buys and social media use, it is still an emerging issue that we are assessing. I can defer to the FBI on their efforts.

Senator HEINRICH. Well, it is not emerging. It emerged. We have been trying to get our hands around this for close to a year now, and we still do not seem to have a plan and that worries me enormously. We have special elections in place. We have gubernatorial elections in place. We are continuing to see this kind of activity, and we need to get a handle on it.

Let me go back to your issue of election infrastructure because as a number of people have mentioned, it has been widely reported that there as cyber intrusion into State-level voting infrastructure. It is my understanding that DHS, before you got there, was aware of those threats well before last year's election but only informed the States in recent months as to the nature of the intrusions in those specific States. Why did it take so long to engage with the subject-matter experts at the State level, and is there a process now in place so that we can get those security clearances that you mentioned in a timely way so that that conversation can head off similar activity next year?

Mr. KREBS. Sir, thank you for the question.

I understand that over the course of the last year or so, officials in each State that was implicated were notified at some level. Now, as we continued to study the issue and got a fuller understanding of how each State has perhaps a different arrangement for elections—in some cases, it is State-local. You have a chief election official. You have a CIO for the State. You have a CIO for the networks. You have a homeland security advisor. As we continued to get our arms around the problem in the governance structure across the 50 States plus territories, we got a better sense of here are the fuller range of notifications we need to make.

So when you think about the notifications of September 22nd, that was a truing up perhaps of each State opening the aperture saying, okay, we let this person know, but we are not letting these additional two or three officials know. So I would not characterize it necessarily as we just let them know then. It was we broadened the aperture, let the responsible officials know, and we gave them additional context around what may have happened.

Senator HEINRICH. I am working on legislation and have been working with the Secretary of State from my State, who is obviously involved in the National Association of Secretaries of State. It is not rocket science. I mean, it is basically building a spread-

sheet of who and at what level. When we see things happen in a given geographic area, you pull out the book and you figure out who you need to be talking to. We need to make sure that that is in place.

Mr. KREBS. Yes, sir. We are actively working that right now.

Senator HEINRICH. Thank you.

Chairman MCCAIN. Senator McCaskill?

Senator MCCASKILL. Thank you.

To reiterate some of the things that I have said previously, but the empty chair is outrageous. We had a foreign government go at the heart of our democracy, a foreign government that wants to break the back of every democracy in the world. A very smart Senator I heard say in this hearing room, who cares who they were going after this time. It will be somebody else next time. I am disgusted that there is not a representative here that can address this.

I also am worried——

Chairman MCCAIN. Can I interrupt, Senator, and just say that we need to have a meeting of the committee and decide on this issue? I believe you could interpret this as a misinterpretation of the privileges of the President to have counsel. He is in charge of one of the major challenges, major issues of our time, and now he is not going to be able to show up because he is, quote, a counselor to the President. That is not what our role is.

Senator MCCASKILL. I mean, I think in any other situation—let us take out this President, take out Russia—this circumstance would not allow to stand by the

United States Senate typically.

Chairman MCCAIN. I agree.

Senator MCCASKILL. You would know more about that than I would. You have been here longer than I have. But I just think this is something that we need—in these times, when there is an issue every day that is roiling this country, we have a tendency to look past things that are fundamental to our oversight role here in the Senate. I am really glad that the chairman is as engaged as he is on this issue, and I look forward to assisting.

Chairman MCCAIN. Well, this should not count against the Senator's time, but we are discussing it and we will have a full committee discussion on it. I thank the Senator.

Senator MCCASKILL. That is great.

Mr. Krebs, I am also worried that we have no nominee for your position. So if the White House reviews this testimony, I hope they will understand that your job is really important. I am not taking sides as to whether or not you are doing a good job or a bad job, but the point is we do not need the word "acting" in front of your name for this kind of responsibility in our government.

Unfortunately, the chairman of the committee that I am ranking on, Homeland Security, has chosen not to have a hearing, believe it or not, on the election interference. So this is my shot and I am hoping that the chairman will be a little gentle with me because I have not had a chance to question on some things.

Why in the world did it take so long to notify the States where there had been an attempt to enter their systems, their voter files?

Mr. KREBS. Again, ma'am, as I mentioned earlier, at some point over the course of the last year, not just September 22nd, an appropriate official, whether it was the owner of an infrastructure, a private sector owner, or a local official, State official, State Secretary, someone was notified.

Senator MCCASKILL. But should not all of the Secretaries of State been notified? I mean, is that not just like a duh?

Mr. KREBS. Ma'am, I would agree. I share your concern. I think over the course of the last several months we, as I mentioned, had a truing up and we have opened a sort of governance per each State. These are the folks that need to be notified of activity.

Senator MCCASKILL. So what is the explanation for a State being told one day that it had been and the next day it had not been? How did that happen?

Mr. KREBS. I understand the confusion that may have surrounded the notifications of September 22nd. I think the way that I would explain that is there was additional context that was provided to the individual States. So in one case perhaps, the election system network may not have been scanned, targeted, whatever it was. It may have been another State system. I would analogize that to the bad guy walking down your street checking your neighbor's door to see if they had a key to get into your house. So it is not always that they are knocking on the network. They may be looking for other ways in through other networks or similarities——

Senator MCCASKILL. That does not change the fact that the Secretaries of State should immediately have been notified in every State whether they had been knocking on a neighbor's door or their own door. The bottom line is—good news—we have a disparate system in our country so it is hard to find one entry point. The bad news is if we do not have clear information going out to these Secretaries of State, then they have no shot of keeping up with the bad guys.

Mr. KREBS. That is right, and going forward, we have that plan in place. We have governance structures. We have notifications. As I mentioned earlier, we have security clearance processes ongoing for a number of officials. We will get them the information they need when they need it and they can act on.

Senator MCCASKILL. Because they do not want to take advantage of what you are offering, which is terrific, that you will come in and check their systems. No mandate, no hook, no expense. I talked to the Secretary of State of Missouri, and he was saying, listen, they are not even talking to us. Now, this was before September.

But I do think somebody has got to take on the responsibility of one-on-one communication with 50 people in the country plus—I do not know who does voting in the territories—as to what is happening, what you are doing, what they are doing. I am not really enamored of the idea of moving all of this to DOD because I think what you guys do with the civilian workforce—I think there would be some reluctance to participate fully if it was directed by DOD.

But the point the chairman makes is a valid one. If you all do not begin a more seamless operation with clear lines of accountability and control, we have no shot against this enemy. None. It worries me that this has been mishandled so much in terms of the

communication between the States that are responsible for the validity of our elections.

Let me talk to you briefly about Kaspersky. I do not even know how you say it. How are you going to make sure it is out of all of our systems?

Mr. KREBS. So, ma'am, a little over a month ago, we did issue a binding operational directive for federal civilian agencies.

Senator MCCASKILL. They get another 90 days to be able to get stuff because you are giving them a long time.

Mr. KREBS. Yes, that is a 90-day process to identify, develop plans to remove. There may be budgetary implications and we have to work through that and then 30 days to execute. We have seen a number of activities in the intervening 30-plus days of actually people going ahead and taking it off.

Senator MCCASKILL. Let me just ask you. Do you think if this happened in Russia, if they found a system of ours that was looking at all of their stuff—do you think they would tell their agencies of government you have 90 days to remove it? Seriously?

Mr. KREBS. I have learned not to predict what the Russians would do.

Senator MCCASKILL. I mean, really but the point I am trying to make is, I mean, why do you not say you have got to do it immediately?

Mr. KREBS. Ma'am, you cannot just rip out a system. There are certain vulnerabilities that can be introduced by just turning a critical antivirus product off. So what we need to do is have a process in place that you can replace with something that is effective. In the meantime, we are able to put capabilities around anything that we do identify to monitor for any sort of traffic.

Senator MCCASKILL. Is the private sector fully aware and are our government contractors fully aware of the dangers of the Kaspersky systems?

Mr. KREBS. Ma'am, we have shared the binding operational directive with a number of our partners, including State and local partners, and working with some of our interagency partners as well. We are sharing risk information.

Senator MCCASKILL. Yes. Is that a little bit like sharing with all the appropriate people at the time but not the Secretaries of State? I mean, I just think there needs to be a really big red siren here. What about government contractors? Is the BOD [Binding Operational Directive]—is it binding on our government contractors?

Mr. KREBS. No, ma'am, it is not. Actually I am sorry. Let me follow up on that to get the specifics.

Senator MCCASKILL. Should it not be?

Mr. KREBS. It would make sense.

Senator MCCASKILL. Since we have more contractors on the ground in Afghanistan than we have troops, would you not think it would be important that we would get Kaspersky out of their systems?

Mr. KREBS. That would be a Department of Defense. My authority only extends to federal civilian agencies.

Senator MCCASKILL. Department of Defense, have you guys told the contractors to get Kaspersky out?

Mr. RAPUANO. We have instructed the removal of Kaspersky from all of the DOD information systems. I will follow up specifically on contractors.

Senator MCCASKILL. I would like an answer on the contractors. Thank you, Mr. Chairman, for your indulgence.

Chairman MCCAIN. Senator Gillibrand?

Senator GILLIBRAND. Thank you, Mr. Chairman.

Your agency, Mr. Krebs, declared that Russian-linked hackers targeted voting systems in 21 States this past election. Why did it take over a year to notify States that their election systems were targeted?

Mr. KREBS. Ma'am, as I have stated, we notified an official within each State that was targeted or scanned. In the meantime, we have offered a series of services and capabilities, including cyber hygiene scans, to every State in the Union and every commonwealth. So not only did we notify the States, granted, there was a broader notification that we subsequently made. But we did make capabilities available to all 50 States and commonwealths.

Senator GILLIBRAND. Are all 50 States using the capabilities that you offered?

Mr. KREBS. I do not have the specific numbers of the States that are using ours, but we have seen a fairly healthy response.

Senator GILLIBRAND. I would like a report on whether all States are using the recommended technology that you offered to them because I think we need to have that kind of transparency given what Senator McCain started this hearing with. I think it is a national security priority. If the States are not doing their jobs well, we need to provide the oversight that is necessary to make sure they do do their jobs well.

Do you believe that making these election cybersecurity consultations optimal is sufficient?

Mr. KREBS. I am sorry. Making them—oh, optional. Optional.

Senator GILLIBRAND. Excuse me. Optional.

Mr. KREBS. You know, fundamentally there are some constitutional questions in play here. What we do in the meantime is ensure that every resource that we have available and out there, that the State and local governments and election systems have the ability to access.

Senator GILLIBRAND. I understand that there is a 9-month wait for a risk and vulnerability assessment. Is that accurate?

Mr. KREBS. We offer a suite of services from remote scanning capabilities, cyber hygiene scans, all the way up to a full-blown vulnerability assessment that sometimes just to execute that vulnerability assessment, because the breadth and depth of the assessment, can actually take a number of weeks, if not months. So we are in the process of looking into whether that 9-month backlog exists and how to ensure, again, that in the meantime, we can provide every other tool needed out to the State and local officials.

Senator GILLIBRAND. I guess what I am trying to get at is are we ready for the next election? Do you believe we are cyber-secure for the next election?

Mr. KREBS. I think there is a lot of work that remains to be done. I think as a country, we need to continue ensuring that we are doing the basics right. Even at the State and local levels, even the

private sector, there are still a lot of basic hygiene activities that need to be done.

Senator GILLIBRAND. I would like a full accounting of what has been done, what is left to be done, and what are your recommendations to secure our electoral system by the next election? I would like it addressed to the entire committee because we just need to know what is out there, what is left.

Senator Graham and I have a bill to have a 9/11 style commission to do the deep dive you are doing, to make recommendations to the Congress on the 10 things we must do before the next election, and then have the authority to come back to us so we can actually implement it because doing it on an ad hoc basis is not sufficient. I am very worried that because there is no accountability and because of the constitutional limitations that you mentioned, that we are not going to hold these States accountable when they have not done the required work.

So we at least need to know what have you succeeded in doing, what is still left to be done, what are the impediments. Is it delays? Is it lack of enough expertise? Is it a lack of personnel? Is it a lack of resources? I need to know because I need to fix this problem.

Mr. KREBS. Yes, ma'am. I will say that we are making significant progress. We have a working relationship, a strong partnership with the State and local election officials, and we are moving forward towards the next election.

Senator GILLIBRAND. Okay.

Mr. Rapuano, in your confirmation hearing, you said that the Russian interference in our election is a credible and growing threat and that Russians will continue to interfere as long as they view the consequences of their actions as less than the benefits that they accrue. Given the likelihood of continued cyber interference in American elections, what are the immediate steps that you are going to take and that the Federal Government should take to restore the integrity of our elections? I know you answered one of the earlier questions with the work we are doing with the National Guard, but I know that you are not necessarily doing all the training necessary or spending the resources to do all the National Guard training consistently with other active duty personnel.

Mr. RAPUANO. Senator, we stand at the ready in terms of the process that DHS has put into place to support all the States with regard to the election system vulnerabilities. To date, we have not been tasked directly to support that effort, but we certainly have capabilities that we could apply to that.

Senator GILLIBRAND. Can I just have your commitment that in the next budget, you will include the full amount needed for the training of these cyber specialists within the National Guard?

Mr. RAPUANO. What I need to do, Senator, is check on the status of our current funding for that effort, and I will get back to you in terms of any deltas.

Senator GILLIBRAND. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Warren?

Senator WARREN. Thank you, Mr. Chairman.

So I want to follow up, if I can, on these questions about the attacks on our voting systems. We know that 21 States faced attacks

on their networks by Russian actors during the run-up to the 2016 election. It seems like the Russians are pretty happy with those efforts, and I do not see any reason to believe that they will not try again.

In fact, Mr. Krebs, your predecessor at Homeland Security recently urged Congress to, quote, have a strong sense of urgency about Russian tampering in the upcoming elections. I know that Homeland Security designated our election system as critical infrastructure earlier this year.

So I would just like to follow up on the question that Senator Gillibrand was asking and what I think I heard you say. Are you confident that our Nation is prepared to fully prevent another round of cyber intrusions into our election systems in 2018 or 2020, Mr. Krebs?

Mr. KREBS. So what I would say is that we have structures in place. This is not an overnight event. We are not going to flip a switch and suddenly be 100 percent secure.

Senator WARREN. So we are not there now.

Mr. KREBS. We are working towards the goal of securing our infrastructure. Yes, ma'am.

Senator WARREN. It is a simple question. We are not there now?

Mr. KREBS. I believe there is work to be done. Yes, ma'am.

Senator WARREN. Okay. So we are not there now.

Can I just ask on maybe some of the specifics? Have you done a State-by-State threat assessment of the cyber environment leading up to the next election?

Mr. KREBS. Are you speaking specific to the election infrastructure or statewide?

Senator WARREN. Election infrastructure.

Mr. KREBS. I would have to check on that.

Senator WARREN. So you do not know whether or not there has been a State-by-State threat assessment?

Mr. KREBS. We have engaged every single State. We are working with their——

Senator WARREN. But my question is actually more specific: a threat assessment for each State on their election infrastructure.

Mr. KREBS. I would have to get back to you on that.

Senator WARREN. Okay.

Are there minimum cyber standards in place for election systems?

Mr. KREBS. We do work with the National Institute of Standards and Technology and the Election Assistance Commission to look at security standards for voting——

Senator WARREN. I understand you work on it. My question is are there minimum cyber standards in place.

Mr. KREBS. There are recommended standards. Yes, ma'am.

Senator WARREN. There are minimum cyber standards.

Mr. KREBS. There are recommended standards. Yes, ma'am.

Senator WARREN. All right. In place.

Are there established best practices?

Mr. KREBS. I believe there are best practices.

Senator WARREN. Those are in place.

Any plans for substantial support for States to upgrade their cyber defenses?

Mr. KREBS. If you are talking about investments——

Senator WARREN. I am.

Mr. KREBS. Okay. That is a different question that I think that we need to have a conversation between the executive branch and Congress about how——

Senator WARREN. Was that a no?

Mr. KREBS. At this point, I do not personally have the funds to assist——

Senator WARREN. So that is a no.

Mr. KREBS. That is a resourcing to States that are grant programs that we can put in place perhaps to improve capability.

Senator WARREN. So you not only do not have the money to do it. Do you any plans—I will ask the question again—for substantial support for States to upgrade their cyber defenses? Do you have plans in place?

Mr. KREBS. We are exploring our options.

Senator WARREN. So the answer is no. You do not have them in place.

Mr. KREBS. We are working on plans. Yes, ma'am. We are assessing what they need.

Senator WARREN. Yes, the answer is no? Okay.

Look, I understand that States have the responsibility for their own elections and also that States run our Federal elections. But I do not think anybody in this room thinks that the Commonwealth of Massachusetts or the City of Omaha, Nebraska should be left by themselves to defend against a sophisticated cyber adversary like Russia. If the Russians were poisoning water or setting off bombs in any State or town in America, we would put our full national power into protecting ourselves and fighting back. The Russians have attacked our democracy, and I think we need to step up our response and I think we need to do it fast.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Peters?

Senator PETERS. Thank you, Mr. Chairman.

Thank you to our witnesses for your testimony today.

I think I would concur with all of my colleagues up here that the number one national security threat we face as a country is the cyber threat. It is one we have to be laser-focused on. I will concur with the chairman others who are very frustrated and troubled by the fact that it does not seem like we have a comprehensive strategy, we do not have a plan to deal with this in a comprehensive way integrating both State and local officials with federal officials, as well as the business sector which is under constant attack.

We know the risk is not just military. It is not just the elections, as significant as that is, because it goes to the core of our democracy, but significant attacks against our economic security, which also goes to the core of our civilization. We have just been hit with an absolutely incredible hack with Equifax that basically has taken now—some actor out there has taken the most private information necessary to open up accounts and to take somebody's identity. You are talking over 100 million people in this country. I cannot think of a worse type of cyber attack.

So, Mr. Smith, my question to you is do you think we will be able to determine who is responsible for that hack?

Mr. SMITH. Yes.

Senator PETERS. When will be able to do that?

Mr. SMITH. I would not want to put a specific time frame on it.

Senator PETERS. Generally.

Mr. SMITH. Generally within maybe 6 or 8 months. That is on the far side.

Senator PETERS. So hopefully within less than that time. So we will be able to identify. I know attribution is always very difficult. Do you believe that we will be able to identify who was responsible?

Then second, do we have to tools to effectively punish those individuals or whoever that entity may be? Those are two separate questions.

Mr. SMITH. Correct and two separate issues.

First, on the attribution point, to get it to a certain destination is easier than the second question, which is imposing significant consequences on an individual or on a specific—if it becomes nation state or associate like that. As you have seen recently, though, with the Yahoo compromise where we have seen a blended threat targeting our businesses and our country where you have criminal hackers working at the direction of Russian intelligence officers, so that is where I become a little more vague as to my answer on specific, would we be able to impose consequences.

Senator PETERS. Which is a significant problem that you cannot answer that, I would think, not you personally—you cannot answer it—that we do not have a plan, we do not have a deterrence plan that says if you do this, these are the consequences for you and they will be significant, particularly if there is a state actor associated with it.

Now, I know, Mr. Rapuano, you mentioned the line. We do not want to actually put a line somewhere because everybody will work up to that line. I think we have a problem now, as we have zero lines right now. So it is like the Wild West out there.

But would you concur that if a state actor, hypothetically a state actor, was behind an Equifax breach that compromised the most personal financial information of over 100 million Americans—would that be over any kind of line that you could see?

Mr. RAPUANO. Sir, I think that the process that we have in play right now in terms of all the reports being submitted in response to the executive order, looking at how we protect critical infrastructure, modernizing IT, develop the workforce, develop deterrence options, looking across those suite of issues, what are our capabilities, what are our vulnerabilities, what are the implications of adversaries that are exploiting those vulnerabilities, that helps inform that doctrine and that also helps inform an understanding of how to best establish what those thresholds are, those deterrence thresholds, what may be too specific to be useful, but what is too vague to be useful as well. We are on the path to developing that.

Senator PETERS. Well, having said that, I think it is a straightforward question, someone who hacks in and steals information from over 100 million Americans and something that compromises their potential identity for the rest of their lives. I would hope the directive would say that that is well over any kind of line.

Mr. RAPUANO. It certainly warrants a consequence, absolutely. Is it an act of war? I think that is a different question, and I think there are a number of variables that go into that. There would be more details that we would be looking at in terms of understanding what the actual impact is, who the actor is, what is our quality and confidence in attribution.

Senator PETERS. Mr. Krebs, you answered some questions related to Kaspersky and taking out that software from the machines of the Federal Government, the United States Government, because of the risk that is inherent there. If the risk is there for the U.S. Government, is it not risky for the average citizen as well to have this software on their computers when we have millions of Americans that have the software and potentially access to their personal information on that computer? Is that not a significant security risk that we should alert the public to?

Mr. KREBS. So risk, of course, is relative. The Department of Homeland Security made a risk assessment for the civilian agencies that we were not willing to have these products installed across our networks. I think that is a pretty strong signal of what our risk assessment was, and we have shared information across the critical infrastructure community and State and locals on that decision.

Senator PETERS. So you say that is an indication of the seriousness of the problem. So the average citizen also will take this software off their system?

Mr. KREBS. I think the average citizen needs to make their own risk-informed decision. Again, the Federal Government has made the decision that this is an unacceptable risk position, and we are instructing agencies to remove at present.

Senator PETERS. Right. Thank you so much.

Chairman MCCAIN. Senator Reed?

Senator REED. Thank you very much, Mr. Chairman.

Just quickly, Mr. Rapuano, following up on Senator Peters? line of questioning, is Cyber Command prepared to engage and defeat an attack on our critical infrastructure in the United States? I know there is an issue here of what is the trigger, but are they prepared to do that right now?

Mr. RAPUANO. So Cyber Command is developing a suite of capabilities against a variety of targets that are—yes, it is inclusive of responding to attack on U.S. critical infrastructure.

Senator REED. The question is—and Senator Peters raised it—what is, for want of a better term, the trigger? You suggested act of war. We are still on sort of the definitional phase of trying to figure out what would prompt this. We have the capability, but the question is under what circumstance do we use it. Is that fair?

Mr. RAPUANO. That is fair. Absolutely.

Senator REED. Thank you.

Chairman MCCAIN. I want to thank the witnesses, and I want to thank you for the hard work you are doing and your candor in helping this committee understand many of the challenges. I must say I appreciate your great work on behalf of the country. But I come back 4 years ago, I come back 2 years ago, I come back 1 year ago. I get the same answers. We put into the defense authorization bill a requirement that there be a strategy, followed by a policy, fol-

lowed by action. We have now, 4 months late, a report that is due before the committee. We have our responsibilities and we are going to carry them out. We have authorities that I do not particularly want to use, but unless we are allowed to carry out our responsibilities to our voters who sent us here, then we are going to have to demand a better cooperation and a better teamwork than we are getting now.

Again, I appreciate very much the incredible service that you three have provided to the country, and I am certainly not blaming you for not being able to articulate to us a strategy which is not your responsibility. The implementation of actions dictated by the strategy obviously is yours.

So when we see the person in charge at an empty seat here today, then we are going to have to react. The committee is going to have to get together and decide whether we are going to sit by and watch the person in charge not appear before this committee. That is not constitutional. We are co-equal branches of government. So I want to make sure that you understand that every member of this committee appreciates your hard, dedicated, patriotic work and what you are dealing with and doing the best that you can with the hand you are dealt.

This hearing has been very helpful to us in assembling—not assembling but being informed as to one of the major threats to America's security. I thank you for that. I thank you for your honest and patriotic work. But we are going to get to this because of the risk to our very fundamentals of democracy among which are free and fair elections.

So is there anything that the Senator from Maine would like to editorialize? He usually likes to editorialize on my remarks.

Senator KING. My mind is racing, but I think prudence dictates no response, Mr. Chairman.

[Laughter.]

Chairman MCCAIN. I thank the witnesses for your cooperation. I thank you for your service to the country.

This hearing is adjourned.

[Whereupon, at 11:53 a.m., the committee was adjourned.]

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR DEB FISCHER

SUPPLY CHAIN SECURITY

1. Senator FISCHER. Beyond the specific actions taken with respect to Kaspersky products, what is your department doing holistically to manage the risks cyber risks associated with companies—particularly IT or telecom companies—that have relationships with foreign governments?

Mr. KREBS. Our supply chain presents a significant source of risk that is being targeted with growing regularity by our most sophisticated adversaries. The acquisition or use of equipment or services from foreign suppliers within U.S. telecommunications networks without a full understanding of the associated risk may undermine the security, integrity, and reliability of those networks. To understand and appropriately mitigate such risks to U.S. telecommunications networks requires significant collaboration with industry, including sharing intelligence related to specific risks to U.S. telecommunications networks and assessments of vulnerabilities.

The Department of Homeland Security (DHS) works in coordination with other federal agencies to address supply chain risk. Several agencies have programs in place to assess supply chain risk of information and communications technology (ICT) purchased by federal agencies. To address these growing risks, the National

Protection and Programs Directorate (NPPD) is launching a Cyber Supply Chain Risk Management (C–SCRM) initiative. The objective of the C–SCRM initiative is to enable stakeholders to make better informed procurement decisions by providing supply chain risk assessments and mitigation recommendations. This initiative is focused on closing known information sharing gaps and supporting DHS's efforts to address supply chain risk for government and private sector entities.

DHS and other interagency partners have engaged with private sector entities to better understand supply chain risk and examine options to mitigating risk. DHS participates in two industry-government working groups addressing increasing concerns regarding business risk and commercial threats. Both of these working groups are making near-term incremental improvements in the identification, communication, and analysis of third party risk-related information.

DHS is a member of the Committee on Foreign Investment in the United States (CFIUS). CFIUS reviews transactions which could result in foreign control of any person engaged in interstate commerce in the United States. As a member of CFIUS, DHS can identify risks to DHS equities arising from CFIUS transactions, including those related to cybersecurity. CFIUS generally takes one of two mitigating actions when unresolved risk is identified: (1) establishment of a binding national security agreement with the parties involved in the transaction, or (2) in rare circumstances, recommend the President prohibit the transaction.

DHS is also a member of Team Telecom, a working group of federal agencies who review FCC applications for new service authorizations, including mergers and acquisitions, involving telecommunications operators with foreign ownership in order to protect U.S. national security, law enforcement, and public safety interests. This allows for dialogue and the sharing of information between DHS and companies with which Team Telecom has mitigation agreements in an effort to address any national security risk that may arise from the FCC granting a new service authorization.

Additionally, DHS implemented a policy to include a requirement to address supply chain risks as a part of efforts related to the management and protection of sensitive DHS systems. DHS requires supply chain risk management principles to be included in the contracting process for all hardware and software to ensure the confidentiality, integrity, and availability of government information.

Mr. RAPUANO. This is a complex challenge because there is a global market for commercial information technology and communications products. Many of the commercial off-the-shelf products used by the DOD can be purchased by foreign governments as well. It is important to distinguish such products produced by a U.S.-based company, or by a company that is headquartered in an allied nation, which can also be purchased by adversaries, from commercial IT products produced by companies based in countries whose interests are not always aligned with United States' interests. One should view such products with caution. The risk associated with global telecom companies is equally complicated due to their global customer base. In each of these cases, DOD has policies in place, or is in the process of putting policies in place, which govern these complex business relationships. The Department has implemented a Trusted Systems and Networks (TSN) strategy as a risk-based approach to address Supply Chain Risk Management (SCRM) concerns for globally sourced information and communications technology being integrated into DOD critical systems and networks. This TSN/SCRM strategy seeks to establish trust and confidence in our critical systems and DOD's ability to execute its missions in a cyber contested environment, around the globe and throughout the system's lifecycle. The DOD Chief Information Officer (CIO) and the Undersecretary of Defense for Acquisition, Technology, and Logistics (AT&L) established DOD policy and regulations (DOD Instruction (DODI) 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (November 12, 2012)), to enable robust SCRM processes across DOD. DODI 5200.44 outlines a SCRM approach for vetting critical components prior to acquiring or integrating them into national security systems (NSS). The multi-discipline approach integrates systems engineering, SCRM, security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, assured services, and information systems security engineering. DOD CIO leads the TSN–Roundtable, which meets quarterly with Service and Agency TSN Focal Points and other stakeholders, to support DOD-wide implementation of DODI 5200.44 by sharing best practices and defining TSN-enterprise capability requirements. In support of the TSN strategy, the Department established enterprise capabilities to support the Services and Agencies in their implementation: The Defense Intelligence Agency established the SCRM Threat Analysis Center to provide supply chain threat assessments to Programs for their critical components. AT&L established the Joint Federated Assurance Center (JFAC) to manage sharing of hardware and software (HW/SW) assurance testing capabilities and foster im-

proved HW/SW test research and development. In addition, the Department has specialized authorities available to address supply chain risks by excluding specific sources. More specifically, section 806 of the NDAA for fiscal year 2011, as amended by section 806 of the NDAA for fiscal year 2013, has been implemented at DFARS Subpart 239.73, "Requirements for Information Relating to Supply Chain Risk." The rule enables DOD components to exclude a source that fails to meet established qualifications standards or fails to receive an acceptable rating for an evaluation factor regarding supply chain risk for information technology acquisitions, and to withhold consent for a contractor to subcontract with a particular source or to direct a contractor to exclude a particular source. DOD is also active in interagency and private sector SCRM efforts. DOD CIO participated in development of National Institute of Standards and Technology (NIST) Special Publication (SP) 800–161 on SCRM Practices for Federal Information Systems and Organizations and co-led with NIST the 2017 update of the Committee on National Security Systems (CNSS) update of the CNSS Directive No. 505, Supply Chain Risk Management. DOD and other interagency partners host quarterly Software & Supply Chain Assurance Forums bringing together industry-academia-government SCRM experts. DOD CIO also continues to engage trade organizations and standards development organizations on "commercially acceptable global sourcing standards."

QUESTIONS SUBMITTED BY SENATOR BEN SASSE

SENATE CYBERSECURITY

2. Senator SASSE. How likely is it that Congressional IT systems have been compromised by hostile foreign intelligence services?

Mr. RAPUANO. I respectfully defer to the DOJ (FBI) and DHS, since the DOD has no jurisdiction or role in the defense of Congressional IT systems, unless a request for technical assistance (RTA) is issued to secure DOD support as part of a cyber incident response effort.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

3. Senator SASSE. Is it possible that foreign intelligence services are sitting on our systems right now undetected?

Mr. RAPUANO. If by saying "our systems" you mean congressional computer networks, I again defer to DOJ to address the question of whether or not foreign intelligence services have intruded onto congressional computer networks.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

CYBERSECURITY DOCTRINE AND STRATEGY

4. Senator SASSE. Where is the Secretary of Defense's cyber strategy?

Mr. RAPUANO. The Department has begun the process to update the 2015 Cyber Strategy. However, it is necessary that this strategy be nested within the National Security, National Military and National Defense Strategies, which are still in development. Therefore, I cannot provide you a specific date when the updated cyber strategy will be released, but I pledge to keep Congress updated as this process progresses.

5. Senator SASSE. Why has this strategy not been produced?

Mr. RAPUANO. The Department continuously assesses the efficacy and scope of its existing Cyber Strategy. Previously, the decision to update our 2011 DOD Cyber Strategy was made in 2014 and resulted in our current DOD Cyber Strategy being published in April 2015. The Department recognizes the need to begin our next cyber strategy update and is building the framework for a new strategy that not only keeps pace with the cyber threat but also addresses congressional concerns. This strategy will be informed by the broader National Security and National Defense Strategies that the Department is currently working with the other departments and agencies. We believe the updated Cyber Strategy must be synchronized with these overarching strategies to produce the most informed and effective final product.

6. Senator SASSE. When will it be completed and when will the SASC be able to review it?

Mr. RAPUANO. Although I cannot provide a specific completion date at this time for the reasons stated above, I can assure the Committee that this is a priority for

the Department's efforts in cyberspace and that substantive work is already underway to produce a final product as soon as possible.

7. Senator SASSE. Mr. Rapuano, what are the fundamentals of cyber deterrence—not cybersecurity per se—but, cyber deterrence? How do we reduce our enemies' desire to conduct cyberattacks against us?

Mr. RAPUANO. Deterring enemies in cyberspace requires intensive interagency policy planning to harmonize (integrate laterally) and synchronize (sequence over time correctly) the use of all instruments of national power to persuade adversaries not to attempt to harm us using cyberspace. First, we must implement world-leading cybersecurity capabilities to make the networks, systems, and information supporting our critical infrastructure and our military forces highly resilient in a cyber-contested environment. This would greatly increase the difficulty encountered by adversaries in mounting successful cyberattacks and could serve to discourage them from making such attempts. At the same time, we must utilize an optimum combination of messaging (e.g., declaratory policy, diplomacy, and capability demonstrations); shaping of the strategic environment in ways that are inhospitable to malicious cyber activities; imposing substantial consequences such as economic penalties for actual cyberattacks attributable to particular actors; law enforcement actions; and building coalitions of like-minded nations to join with us in these efforts. In addition, increasing our capability to detect, block, and disrupt or subvert malicious cyber threat activities will minimize any adversary's success, making such activities less attractive and more costly. Exposing cyber threat activity as unacceptable behavior, and attaching civil, criminal or monetary or trade sanctions when we have adequate attribution can create disincentives and hesitation on the part of our adversaries. Establishing and enforcing a cyber behavior threshold with escalating severity will build structure of predictable and unpredictable consequences that will help shape cyber threat actor intentions and actions.

8. Senator SASSE. How is DOD doing in building our nation's cyber deterrence doctrine?

Mr. RAPUANO. Deterring malicious behavior in cyberspace requires a whole-of-government approach. Consequently, DOD is actively participating in interagency efforts to develop a report on the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats, as required by the President's Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. That report, when completed, will shape our deterrence activities in support of national level cybersecurity policy, which will entail numerous follow-on implementation efforts by all interagency players. As DOD formulates its own Department-level cyber deterrence doctrine, an effort currently underway, we will seek to ensure that it is compatible with, and supports, the emerging national-level strategy.

THREAT OF CYBER ATTACK

Senator SASSE. Mr. Smith, are there any ongoing efforts by Russia, China, North Korea, or any other State to digitally target U.S. critical infrastructure or systems?

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

9. Senator SASSE. On a scale of 1–10 (10 being the most dangerous), how would you rank the current cyber threat against the U.S.?

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

10. Senator SASSE. What cyber threat or vulnerability are you most concerned about these days?

Mr. KREBS. There are a range of high priority risk areas based on the current threat environment. Adversaries continue to test our critical infrastructure, and as a result we are focusing efforts on the interconnectedness and communications reliance of our nation's critical infrastructure, particularly those services that underpin the essential functions of our economy and way of life. Over the past year, Americans saw advanced persistent threat actors, including hackers, cyber criminals, and nation-states increase the frequency and sophistication of these attacks. Our adversaries have been developing and using advanced cyber capabilities to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets and threaten our democracy through attempts to manipulate elections.

We are working with our partners in the Government and private sector to defend against and mitigate the risk posed by our adversaries.

Senator SASSE. All Witnesses: Please provide a one-word answer to the following question:

11. Is the nation's cyber vulnerability level "acceptable" (meaning we have the threat under control), is it "concerning" (meaning the threat is rising and may soon pose a significant risk to our national interests and our way of life), or is it "critical" (meaning the threat already poses a significant risk to our national interests and our way of life)?

Mr. Joyce did not respond in time for printing. When received, answer will be retained in committee files.

Mr. RAPUANO. It is difficult to state definitively the Nation's level of vulnerability in cyberspace at any one moment. However, the evolving nature of the cyber threat and the pace and scope at which the U.S. Government is witnessing cyber incidents against key sectors of the U.S. economy and infrastructure highlight the continued need to address our Nation's cyber vulnerabilities as a priority. As highlighted in my testimony, it is not likely that we can address every vulnerability and thus must prioritize efforts to protect the most critical assets and manage risk strategically. In the defense industrial sector, this threat already poses a significant risk to the U.S. warfighting capability today and in the future. Recent changes in acquisition regulations regarding protection of controlled defense information on contractor information systems will provide some risk reduction, as will the emphasis on countering insider threats. The President's Cyber Executive Order directs the Executive Branch to provide such an updated framework.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

Mr. KREBS. Cyber threats remain one of the most significant strategic risks to the United States, threatening our national security, economic prosperity, and public health and safety. The level of vulnerability varies across sectors and fluctuates based on new technology that is acquired. Instead of focusing on a general score, DHS is committed to defending federal networks and ensuring the security of cyberspace and critical infrastructure.

12. Senator SASSE. What concrete steps need to be taken to reduce our cyber risk to an acceptable level?

Mr. Joyce did not respond in time for printing. When received, answer will be retained in committee files.

Mr. RAPUANO. Individual cyber risks are assessed by evaluating the combination of criticality, vulnerability, and threat variables. DOD assesses the cyber risk by following the National Institute of Standards and Technology (NIST) Risk Management Framework, which defines risk as a "measure of the extent to which an entity is threatened by a potential circumstance or event, and a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." DOD is taking a number of concrete steps to reduce our cyber risk to an acceptable level, including conducting cyber assessments of its critical assets, enhancing cyber defensive capabilities, updating contracting rules to improve accountability and responsibility for protection of DOD data within the Defense Industrial Base (DIB), updating information systems security requirements, developing policies to support cyber damage assessment processes, and focusing on protection of the Department's critical acquisition programs and technologies. In addition, DOD is in the process of conducting cyber vulnerability assessments of our major weapon systems and our critical infrastructure, in response to section 1647 of the fiscal year 2016 NDAA and section 1650 of the fiscal year 2017 NDAA.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

Mr. KREBS. Safeguarding and securing cyberspace is a core homeland security mission. Malicious cyber actors target the paths of least resistance, lowest effort for the biggest payoff, and simplicity. Many information technology system compromises exploit basic vulnerabilities such as: email phishing, insecure password practices, default and improper configuration, and poor patch management. Continuing to address these basic vulnerabilities will make significant progress in reducing the Nation's cybersecurity risk.

Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, recognizes that effective cybersecurity requires entities to identify, detect, respond, and if necessary, recover from cyber intrusions. We are fully engaged in outreach to stakeholders to provide cybersecurity threat informa-

tion and highlight the need to prioritize and manage cybersecurity risks. We also promote the standardization of information technology and cybersecurity capabilities to control costs and improve asset management, and provide support to improve incident detection, reporting and response capabilities.

Section 9 of Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, states that DHS "shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." Further, section 9 states, "the Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis." The National Protection and Programs Directorate (NPPD) executes this program using a collaborative approach with expertise from public and private sector partners and Sector-Specific Agencies.

Identification supports both critical infrastructure needs and national security objectives by providing the Federal Government with the ability to more effectively disseminate specific and targeted cybersecurity threat information to identified cyber-dependent critical infrastructure. This then supports the prioritization, as appropriate, of government resources and programs available to identified cyber-dependent critical infrastructure, helping improve the Government's understanding of those systems or assets whose incapacity or disruption would have catastrophic consequences. This understanding helps inform the Government's planning, protection, mitigation and response efforts provided in partnership with impacted state, local, territorial, tribal and private sector entities in the event of a cyber incident.

QUESTIONS SUBMITTED BY SENATOR JEANNE SHAHEEN

REMOVAL OF KASPERSKY SOFTWARE FROM GOVERNMENT SYSTEMS

13. Senator SHAHEEN. Secretary Krebs, Kaspersky Lab partners with many well-known companies that specialize in areas beyond anti-virus protection. How are you ensuring that every bit of Kaspersky software whether it be on government computers, networks, and TVs is completely removed from U.S. systems within 90 days (according to the DHS directive)?

Mr. KREBS. On September 13, 2017, the Acting Secretary of Homeland Security issued Binding Operational Directive (BOD) 17–01: Removal of Kaspersky-Branded Products. BOD 17–01 instructs federal agencies to identify and report to the Department of Homeland Security (DHS) by October 13, 2017, the use or presence of Kaspersky Lab-branded products on federal information systems. This process has identified the use of Kaspersky Lab-branded products on some systems at some agencies. Those agencies also developed plans to remove such products as required by the BOD.

DHS provided an opportunity for Kaspersky Lab to submit a written response addressing the Department's concerns. This opportunity provided the company a full opportunity to inform the Acting Secretary of any evidence, materials, or data that may be relevant. This opportunity was also made available to any other entity that claims its commercial interests are directly impacted by the directive.

14. Senator SHAHEEN. Secretary Krebs, what is the standard applied to agencies working to successfully remove all Kaspersky products from their systems?

Mr. KREBS. On September 13, 2017, the Acting Secretary of Homeland Security issued Binding Operational Directive (BOD) 17–01: Removal of Kaspersky-Branded Products. BOD 17–01 instructs federal agencies to identify and report to the Department of Homeland Security (DHS) by October 13, 2017, the use or presence of Kaspersky Lab-branded products on federal information systems. This process has identified the use of Kaspersky Lab-branded products on some systems at some agencies. Those agencies also developed plans to remove such products as required by the BOD.

DHS provided an opportunity for Kaspersky Lab to submit a written response addressing the Department's concerns. This opportunity provided the company a full opportunity to inform the Acting Secretary of any evidence, materials, or data that may be relevant. This opportunity was also made available to any other entity that claims its commercial interests are directly impacted by the directive.

15. Senator SHAHEEN. Secretary Krebs, do you plant to consult with this Committee on the directive's progress after the initial 60-day review?

Mr. KREBS. On September 13, 2017, the Acting Secretary of Homeland Security issued Binding Operational Directive (BOD) 17–01: Removal of Kaspersky-Branded

Products. BOD 17–01 instructs federal agencies to identify and report to the Department of Homeland Security (DHS) by October 13, 2017, the use or presence of Kaspersky Lab-branded products on federal information systems. This process has identified the use of Kaspersky Lab-branded products on some systems at some agencies. Those agencies also developed plans to remove such products as required by the BOD.

DHS provided an opportunity for Kaspersky Lab to submit a written response addressing the Department's concerns. This opportunity provided the company a full opportunity to inform the Acting Secretary of any evidence, materials, or data that may be relevant. This opportunity was also made available to any other entity that claims its commercial interests are directly impacted by the directive.

OTHER AGENCIES

16. Senator SHAHEEN. Secretary Krebs, have other agencies been successful in identifying and removing Kaspersky products on their information systems?

Mr. KREBS. On September 13, 2017, the Acting Secretary of Homeland Security issued Binding Operational Directive (BOD) 17–01: Removal of Kaspersky-Branded Products. BOD 17–01 instructs federal agencies to identify and report to the Department of Homeland Security (DHS) by October 13, 2017, the use or presence of Kaspersky Lab-branded products on federal information systems. This process has identified the use of Kaspersky Lab-branded products on some systems at some agencies. Those agencies also developed plans to remove such products as required by the BOD.

DHS provided an opportunity for Kaspersky Lab to submit a written response addressing the Department's concerns. This opportunity provided the company a full opportunity to inform the Acting Secretary of any evidence, materials, or data that may be relevant. This opportunity was also made available to any other entity that claims its commercial interests are directly impacted by the directive.

QUESTIONS SUBMITTED BY SENATOR RICHARD BLUMENTHAL

ELECTION INTERFERENCE

17. Senator BLUMENTHAL. Mr. Rapuano, Mr. Smith, and Mr. Krebs, do you agree that Russia must pay a steeper price for its cyberattacks and interference in our election? Do you agree that our actions so far have not made Russia realize that they have more to lose than gain with their behavior?

Mr. RAPUANO. Russia is a determined adversary with advanced cyber capabilities that it is willing to employ to advance Russia's national interests. Although I think the United States response to Russian election interference clearly communicated how seriously we took their actions, I am not convinced that it was sufficient to deter Russia from undertaking similar activities in the future. If Russia views the benefits of its actions to be greater than the risks, its unacceptable conduct is likely to continue. All that said, no single U.S. Government action, and no single DOD activity, will successfully counter Russia's malign influence activities. The United States must approach this as a sustained long-term campaign that leverages all instruments of national power to deter, counter, and when required, respond to Russia's attempts to undermine United States national interests and values.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

Mr. KREBS. The U.S. Government seeks to leverage our various authorities and capabilities to secure vital systems and assets, improve resilience against cyber incidents, and quickly respond to and recover from incidents when they occur. Regarding Russia or any other state or non-state actor, deterrence is an important component of national efforts to change the behaviors of malicious cyber actors and to protect information and information systems, including critical infrastructure, from harm. The foundation of our deterrence and broader cybersecurity efforts includes securing our own systems before an adversary acts thereby making exploitation of U.S. infrastructure more difficult and costly. This denies malicious cyber actors any benefit to less sophisticated attempts at intrusion and reduces benefits to more sophisticated attacks. Deterrence by denial requires a whole of Government, and indeed whole of Nation, approach that is coordinated with our private sector, state and local, and international partners across all areas of national preparedness.

The Department of Homeland Security (DHS) supports and enables the security and resilience of non-federal entities through its network protection efforts. Network protection includes providing entities with information and technical capabilities they can use to secure their networks, systems, assets, information, and data, by

providing technical assistance and risk management support as well as recommendations on security and resilience measures to facilitate information security and strengthen information systems against cybersecurity risks and incidents. These efforts are carried out by DHS's National Protection and Programs Directorate, which includes the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC operates at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities.

Network protection is only one component of the Federal Government's overall effort to deter malicious cyber actors. DHS's law enforcement agencies and intelligence offices play a key role as well. Additionally, our interagency partners make important contributions to overall deterrence efforts through proactive risk reduction efforts, sanctions, diplomatic actions, and offensive operations.

This year DHS stood up an Election Task Force (ETF) to improve coordination with and support to our stakeholders. NPPD is leading the task force, which includes personnel from across the Department, as well as interagency partners. NPPD is working with interagency partners to address risk to elections, including countering influence campaigns.

18. Senator BLUMENTHAL. Mr. Rapuano, Mr. Smith, and Mr. Krebs, what is being done to prevent Russia—or any other state or non-state actor—from conducting influence campaigns designed to disrupt our elections?

Mr. RAPUANO. Consistent with Mr. Krebs' testimony, the Federal government is engaging with domestic authorities to ensure they that have the information and resources necessary to secure their information systems, databases, and other related election infrastructure. Although DOD is not directly involved in these activities, it is prepared to support DHS and the FBI in these efforts, if requested and where appropriate. Consistent with DOD's mission, DOD seeks actively to characterize adversary threats to provide advance warning and, when directed, employ potential response options to counter adversary cyber activities. Fundamentally, Russia's complex information operation targeted United States citizens by exploiting existing political and social divisions, and the digital media environment. It's important to note that developing and fielding state-of-the-art cyber defenses alone will be insufficient to counter ongoing or future nation-state influence operations. Building our nation's resiliency to these types of actions will require a whole of nation response that involves working with the private technology sector, educating the public, increasing awareness, exposing malicious actions, etc. Many such actions exceed DOD authorities or resources.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

Mr. KREBS. The U.S. Government seeks to leverage our various authorities and capabilities to secure vital systems and assets, improve resilience against cyber incidents, and quickly respond to and recover from incidents when they occur. Regarding Russia or any other state or non-state actor, deterrence is an important component of national efforts to change the behaviors of malicious cyber actors and to protect information and information systems, including critical infrastructure, from harm. The foundation of our deterrence and broader cybersecurity efforts includes securing our own systems before an adversary acts thereby making exploitation of U.S. infrastructure more difficult and costly. This denies malicious cyber actors any benefit to less sophisticated attempts at intrusion and reduces benefits to more sophisticated attacks. Deterrence by denial requires a whole of Government, and indeed whole of Nation, approach that is coordinated with our private sector, state and local, and international partners across all areas of national preparedness.

The Department of Homeland Security (DHS) supports and enables the security and resilience of non-federal entities through its network protection efforts. Network protection includes providing entities with information and technical capabilities they can use to secure their networks, systems, assets, information, and data, by providing technical assistance and risk management support as well as recommendations on security and resilience measures to facilitate information security and strengthen information systems against cybersecurity risks and incidents. These efforts are carried out by DHS's National Protection and Programs Directorate, which includes the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC operates at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities.

Network protection is only one component of the Federal Government's overall effort to deter malicious cyber actors. DHS's law enforcement agencies and intelligence offices play a key role as well. Additionally, our interagency partners make important contributions to overall deterrence efforts through proactive risk reduction efforts, sanctions, diplomatic actions, and offensive operations.

This year DHS stood up an Election Task Force (ETF) to improve coordination with and support to our stakeholders. NPPD is leading the task force, which includes personnel from across the Department, as well as interagency partners. NPPD is working with interagency partners to address risk to elections, including countering influence campaigns.

19. Senator BLUMENTHAL. Mr. Rapuano, Mr. Smith, and Mr. Krebs, how do you define a cyberattack? What constitutes an act of war?

Mr. RAPUANO. As is the case in all other domains, a determination of whether a malicious cyber activity constitutes an act of war (equivalent to an "armed attack" or use of force) or a cyberattack warranting a U.S. response is made on a case-by-case basis by the President, regardless of the actor. It is the context and consequence, not the means, of an attack that matter most. Malicious cyber activities could result in death, injury or significant destruction, and any such activities likely would be regarded with the utmost concern and could well be considered an armed attack or use of force. It is also important to note that malicious cyber activity does not need to be deemed an "act of war" or an "armed attack" to warrant a response. If a decision is made by the President to respond to a cyberattack on U.S. interests, the United States reserves the right to respond at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

Mr. KREBS. In December 2016, the Department of Homeland Security led development of the National Cyber Incident Response Plan, in coordination with the Department of Justice, the Department of Defense, Sector Specific Agencies, other interagency partners, state and local governments, and private sector critical infrastructure entities. While this plan was not intended to define terms such as cyberattack or act of war, it did establish a common framework for understanding the severity of a cyber incident. Included in this plan is a cyber incident severity schema established by the Federal Government's cybersecurity centers, in coordination with departments and agencies with a cybersecurity or cyber operations mission. The schema established a framework for describing the severity of cyber incidents affecting the Homeland, U.S. capabilities, or U.S. interests, providing a common view of the severity of a given incident, urgency required for responding to a given incident, seniority level necessary for coordinating response efforts, and level of investment required for response efforts. The schema has proven helpful in coordinating interagency response efforts during previous cyber incidents. Additional information regarding the National Cyber Incident Response Plan and related schema can be found online at: *https://www.us-cert.gov/ncirp.*

20. Senator BLUMENTHAL. Mr. Rapuano, Mr. Smith, and Mr. Krebs, in January, former DHS Secretary Johnson designated election infrastructure as critical infrastructure. Last month we learned Russia tried to access voter information in over 20 states, including CT. What concrete steps have been taken to fortify our election systems? What will be done differently for the 2018 elections?

Mr. RAPUANO. The Department of Defense respectfully defers to the Department of Homeland Security (DHS) as the Executive Branch entity with purview over election-related cybersecurity.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

Mr. KREBS. The designation of election infrastructure as a critical infrastructure subsector in January 2017 by the Department of Homeland Security (DHS) has formalized the prioritization of assistance from the Federal Government for state, local, tribal, and territorial governments, and private sector entities in their efforts to reduce risks to election infrastructure. Participation with the Federal Government, as part of this subsector, is voluntary. This dynamic is consistent with the engagements between the Federal Government and other previously established critical infrastructure sectors and subsectors, including the chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, material, and waste, transportation systems, and water and wastewater systems sectors.

This year DHS stood up an Election Task Force (ETF) to improve coordination with and support to our stakeholders. DHS's National Protection and Programs Directorate (NPPD) is leading the task force, which includes personnel from across the Department, as well as interagency partners.

The ETF focuses efforts on:

- Improving communication with election officials in order to provide understanding and actionable information to assist them in strengthening the security of their election infrastructure as it relates to cybersecurity risk.
- Ensuring coordination of these activities across the Department.
- Increasing coordination with intelligence community and law enforcement partners.
- Supporting regional efforts to ensure they are coordinated and provide election officials with the support and expertise they need.

DHS is committed to improving the effectiveness of information sharing protocols, both from DHS and among state officials. As the sector-specific agency, DHS is providing overall coordination guidance on election infrastructure matters to subsector stakeholders. As part of this process, the Election Infrastructure Subsector Government Coordinating Council (GCC) was established. The Election Infrastructure Subsector GCC is a representative council of federal, state, and local partners with the mission of focusing on sector-specific strategies and planning. The GCC structure is established under the department's authority to provide a forum in which the Government and private sector entities can jointly engage in a broad spectrum of activities to support and coordinate critical infrastructure security and resilience efforts. It is used in each of the critical infrastructure sectors established under Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience.

FOREIGN SOFTWARE

21. Senator BLUMENTHAL. Mr. Rapuano and Mr. Krebs, last month, DHS banned Moscow-affiliated company Kaspersky Labs software products and services from being used by all government agencies. DHS will give agencies 90 days to discontinue use of Kaspersky products. Senator Shaheen worked to include a provision in this year's Senate-passed NDAA to prohibit the use of Kaspersky products across the Government as well. What efforts has DOD and DHS taken to identify foreign software products being used within government agency systems?

Mr. RAPUANO. DOD has processes in place to systematically identify software products being used in its national security systems that present counterintelligence risk, foreign or domestic. While DOD remains concerned about software that is developed in a foreign country, that concern is heightened when a foreign government may have undue influence on the development of software (e.g., inject or modify code). Additionally, software is often developed in many places around the globe and is often based on pre-existing software modules. One of the major tenets of DOD's Trusted Systems and Networks (TSN) Strategy and policy (DOD Instruction 5200.44) is the use of all-source intelligence analysis on critical components of DOD's National Security Systems. The all-source intelligence analyses, performed by the Defense Intelligence Agency's Supply Chain Risk Management (SCRM) Threat Analysis Center, performs a deep analysis into the supply chain of the subcomponents that make up a particular product, including embedded software. The Joint Federated Assurance Center also coordinates the sharing of hardware and software testing capabilities to assess for vulnerabilities in these products. Once a specific threat is identified, DOD has processes to identify and mitigate the threat posed by foreign software. DOD queries contract tools (System for Award Management (SAM); Federal Procurement Data System (FPDS); Electronic Document Access (EDA); and Wide Area Workflow (WAWF)) to identify where DOD has procured software of interest. DOD can also initiate scans of software on networks. DOD is continuing to enhance our capability to investigate our global supply chain and is currently investigating use of commercial due-diligence tools to identify strategic alliances between foreign sources with potential foreign intelligence entity influence and original equipment manufacturers.

Mr. KREBS. On September 13, 2017, the Acting Secretary of Homeland Security issued Binding Operational Directive (BOD) 17–01: Removal of Kaspersky-Branded Products. BOD 17–01 requires federal agencies to identify and report to the Department of Homeland Security (DHS), by October 13, 2017, the use or presence of Kaspersky Lab-branded products on federal information systems. This process has identified the use of Kaspersky Lab-branded products on some systems at some agencies. Those agencies either removed the products or are in the process of removing the products.

22. Senator BLUMENTHAL. Mr. Rapuano and Mr. Krebs, what threats do foreign goods present to our cyber security?

Mr. RAPUANO. U.S. competitors and adversaries increasingly participate in the information and communications technology supply chain, making it increasingly untrustworthy. There are supply chain threats to our systems at every point of the

acquisition lifecycle: an adversary may maliciously introduce unwanted function or otherwise subvert the design, integrity, manufacturing, product, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such capabilities. Adversaries may also exploit vulnerabilities in systems and those in the Defense Industrial Base (DIB) partners to obtain DOD information. Once a specific threat is identified, DOD has processes to identify and mitigate the threat posed by foreign software. DOD queries contract tools to include System for Award Management (SAM); Federal Procurement Data System (FPDS); Electronic Document Access (EDA); and Wide Area Workflow (WAWF) to identify where DOD has procured software of interest. DOD can also initiate scans of software on networks. DOD is continuing to enhance our capability to investigate our global supply chain and is currently investigating use of commercial due-diligence tools to identify strategic alliances between foreign sources with potential FIE influence and original equipment manufacturers.

Mr. KREBS. The globalization of the information technology supply chain introduces additional risks to product integrity and software and hardware assurance. Goods which are produced in foreign countries or domestically within the U.S. have the potential for vulnerabilities; however there are growing concerns associated with foreign ownership, control, manipulation, or influence of certain products. It is critical to understand that the problem is not a simple function of geography. Products with known cyber vulnerabilities or exploitable weaknesses are also produced by domestic companies.

23. Senator BLUMENTHAL. Mr. Rapuano and Mr. Krebs, are agencies using Kaspersky still facing a security concern as they've been given 90 days from the DHS directive to discontinue use?

Mr. RAPUANO. DOD is following the principles associated with the DHS Binding Operational Directive to identify and remove Kaspersky Lab software. As long as the software is in use on agency networks and mitigations have not been taken, they are at risk of Kaspersky having access to files and elevated privileges on computers on which the software is installed. This information could be used to compromise federal information and information systems.

Mr. KREBS. On September 13, 2017, the Acting Secretary of Homeland Security issued Binding Operational Directive (BOD) 17–01: Removal of Kaspersky-Branded Products. BOD 17–01 requires federal agencies to identify and report to the Department of Homeland Security (DHS), by October 13, 2017, the use or presence of Kaspersky Lab-branded products on federal information systems. This process has identified the use of Kaspersky Lab-branded products on some systems at some agencies. Those agencies either removed the products or are in the process of removing the products.

24. Senator BLUMENTHAL. Mr. Rapuano and Mr. Krebs, what additional authorities do you need to secure our networks?

Mr. RAPUANO. The Department currently assesses that it has all the authorities it needs from Congress to achieve its missions in cyberspace. However, DOD constantly evaluates its ability to conduct these missions, and I will reach out to the Committee should additional authorities be needed to secure DOD networks.

Mr. KREBS. The Department of Homeland Security (DHS) appreciates the opportunity to continue its work with Congress to fully authorize and fund DHS's efforts to safeguard and secure cyberspace, a core homeland security mission. The National Protection and Programs Directorate (NPPD) at DHS leads the Nation's efforts to enhance the security and resilience of our cyber and physical infrastructure. DHS will continue to work with Congress regarding legislation that would mature and streamline NPPD's authorities and rename our organization to clearly reflect our essential mission and role in securing cyberspace, in a manner that protects privacy and civil liberties. DHS strongly supports this much-needed effort.

25. Senator BLUMENTHAL. Mr. Rapuano and Mr. Krebs, how are you ensuring the commercial sector is adequately protecting its networks so that highly sensitive information linked to DOD is protected?

Mr. RAPUANO. With the release of the Binding Operational Directive (BOD), DHS has encouraged private sector entities and the public to assess their cybersecurity risk and to take actions they deem appropriate. DOD has briefed Information Technology Sector and Defense Industry Base members on the threat associated with Kaspersky's antivirus products over the past year (prior to the BOD release) through formal public-private partnerships. In a September 28, 2017, notice to National Industrial Security Program (NISP) Contractors with Authorized Information Systems (i.e., classified information systems), the Defense Security Service (DSS) di-

rected the removal of all Kaspersky Labs software or hardware from classified information systems under DSS cognizance.

The DSS uses the National Institute of Standards and Technology Risk Management Framework (RMF) to oversee the protection of DOD classified information and technologies. RMF provides companies a standard and comprehensive structure for managing cybersecurity risks across their enterprises, enabling them to devise, implement and monitor security measures to address any identified risks. Industry networks that process or hold classified information operate under DSS authority and oversight, use the National Security Agency-approved encryption, and function independent of the unclassified internet. DSS continually collects information from U.S. Government organizations, cleared contractors, and commercial sources on threats to that information. Those threats may operate directly against the information system or against unclassified networks that give the adversary information concerning classified programs it can use to determine, define, and execute intelligence activities through cyber and human means.

DOD continues to engage and share information with direct support contractors on cyber security and supply chain risks. DOD has a range of activities that include both regulatory and voluntary programs to improve the collective cybersecurity of the nation and to protect sensitive DOD information on private sector networks. These activities include securing DOD's information systems and networks, codifying cybersecurity responsibilities and procedures for the acquisition workforce in defense acquisition policy, implementing contractual requirements through the Defense Federal Acquisition Regulation Supplement (DFARS), sharing cyber threat information where appropriate through DOD's voluntary Defense Industrial Base (DIB) Cybersecurity Program, and leveraging National Institute of Standards and Technology (NIST) security standards.

In October 2016, DOD updated DFARS Clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. DFARS Clause 252.204–7012, required in all contracts except for contracts solely for the acquisition of COTS items, requires contractors to provide "adequate security" for covered defense information that is processed, stored, or transmitted on the contractor's internal information system or network. To do so, the clause requires contractors to, at a minimum, implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," not later than December 31, 2017. The clause also requires defense contractors to report to DOD cyber incidents that affect covered defense information or the contractor's ability to provide operationally critical support; to submit malicious software associated with the cyber incident; to facilitate damage assessment processes; and to flow down the clause to subcontractors when the contract performance will involve covered defense information or operationally critical support. Since publication of the final rule in October of 2016, the Department has embarked on an extensive outreach effort to inform and assist the defense industrial base in implementing DFARS Clause 252.204–7012 and NIST SP 800–171.

Since 2008, DOD has partnered with companies in the Defense Industrial Base (DIB) through the cyber threat information sharing DIB Cybersecurity (CS) program. This voluntary program has add steadily expanded and has matured as a model for public-private cyber collaboration. The program is codified as a permanent DOD program in 32 Code of Federal Regulations part 236. During fiscal year 2017 the DIB CS program expanded by 37 percent during with participants now totaling over 250 companies. DOD's approach to safeguarding DOD and DIB controlled unclassified information DOD is intended to raise the bar on cybersecurity in the DIB and better protect unclassified DOD information residing in or transiting DIB networks or information systems.

Mr. KREBS. The Department of Homeland Security (DHS) supports and enables the security and resilience efforts of the commercial sector through its network protection efforts. Network protection includes providing organizations with information and technical capabilities they can use to secure their networks, systems, assets, information, and data, by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. These efforts are carried out by DHS's National Protection and Programs Directorate, which includes the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC operates at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities. DHS also works with government partners, including the National Institute of Standards and Technology, to support the adoption of the NIST Framework for Improving Critical Infrastructure cybersecurity, which is a voluntary, flexible, risk-based approach an organization can use to manage its cybersecurity risks.

RUSSIAN INTERFERENCE WITH NATO TROOPS

26. Senator BLUMENTHAL. Mr. Rapuano, earlier this month, the Wall Street Journal reported that Russia is targeting NATO troops' personal smartphones in an effort to intimidate them, as well as glean operational information. What is being done to protect our servicemembers and counter Russia's intrusions? What are you doing to educate our servicemembers?

Mr. RAPUANO. The Department of Defense (DOD) is mitigating the risk of Russian targeting of the personal smartphones of NATO personnel through a combination of cybersecurity training and procedural controls. DOD continues to update and disseminate its Identity Awareness, Management, and Protection Guide to enable service members to harden their personal devices from any malicious activity, whether by a nation-state or non-state actor. For Force Protection purposes, DOD also provides guidance to its personnel on how to protect their personally identifiable information. Additionally, the DOD continues to integrate cybersecurity best practices related to personal devices into its annually required cybersecurity/information assurance refresher training. Procedurally, DOD continues to enforce and improve procedural controls for where and how service members utilize their personal smartphones in and around military sites and facilities. DOD also is considering a range of options to ensure that we are best postured against this threat as it evolves.

27. Senator BLUMENTHAL. Mr. Rapuano, while Russia's targeting of servicemembers for intelligence is not new, personal smartphones provide significantly more knowledge about a person than was easily accessible in the past. In what ways are you ensuring this vulnerability is not having an impact on our efforts in Eastern Europe?

Mr. RAPUANO. The Department of Defense (DOD) is mitigating the risk of Russian targeting of the personal smartphones of NATO personnel through a combination of cybersecurity training and procedural controls. DOD continues to update and disseminate its Identity Awareness, Management, and Protection Guide to enable service members to harden their personal devices from any malicious activity, whether by a nation-state or non-state actor. For Force Protection purposes, DOD also provides guidance to its personnel on how to protect their personally identifiable information. Additionally, the DOD continues to integrate cybersecurity best practices related to personal devices into its annually required cybersecurity/information assurance refresher training. Procedurally, DOD continues to enforce and improve procedural controls for where and how service members utilize their personal smartphones in and around military sites and facilities. DOD also is considering a range of options to ensure that we are best postured against this threat as it evolves. The DOD has also emphasized training for service members regarding social media use; this training includes education of privacy and security settings as well as operational security considerations before posting, tagging, etc. to social media sites.

28. Senator BLUMENTHAL. Mr. Rapuano, what precautions are being taken to address the risk of a compromised phone being able to collect information from its surroundings?

Mr. RAPUANO. The Department of Defense continues to integrate personal device cybersecurity best practices within its annually required cybersecurity/information assurance refresher training. Procedurally, DOD continues to enforce and improve procedural controls for where and how service members utilize their personal smartphones in and around military sites and facilities. This includes the powering off and secured storage of personal smart phones before entering secure official work spaces. These procedures are also being evaluated and considered for other military sites and areas, including official unclassified work spaces.

QUESTIONS SUBMITTED BY SENATOR TIM KAINE

INTERAGENCY INTERNATIONAL CYBER COORDINATION

29. Senator KAINE. Who is your direct peer at the Department of State that you consult with regularly or would consult with on international cyber threats and do you believe it is within U.S. strategic interests to move the State Department's Cyber Coordinator office under the Bureau of Economic and Business Affairs, from a national security standpoint?

Mr. RAPUANO. My current counterpart at the State Department is the Assistant Secretary of State for Economic and Business Affairs. I believe the State Depart-

ment plays an indispensable role in promoting U.S. interests in cyberspace. I would respectfully defer the State Department about how it can and should be best organized to play this role.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

Mr. KREBS. The Department of Homeland Security (DHS) works closely with the Department of State, and other interagency partners, as well as foreign governments, regional and international organizations, the private sector and civil society, to foster collaborative efforts to accomplish national and homeland security objectives and to advance an open, interoperable, secure, and reliable cyberspace. At the Under Secretary level, this work is done by the State Department's Under Secretary for Economic Growth, Energy and Environment. NPPD works closely with the State Department's Deputy Assistant Secretary for Cyber and International Communications and Information Policy. DHS defers to the State Department on how best to organize itself to carry out its authorities. Regardless of organizational structure, DHS will continue to work closely with all appropriate offices at the State Department in order to achieve our mission of safeguarding and securing cyberspace. The State Department serves a key role in enabling DHS's international efforts.

30. Senator KAINE. A 2013 Council on Foreign Relations Task Force report titled Defending an Open, Global, Secure, and Resilient Internet, written by a bipartisan group of officials, recommended elevating State Department's Cyber Coordinator position to an Assistant Secretary position and to be the lead of a cyber bureau. Do you feel that Economic and Business Affairs is in an appropriate place, with effective lines of communication with your offices to ensure that you will have all of State Department's equities with a peer level input when you consider options to respond to an international cyberattack?

Mr. RAPUANO. I believe the State Department plays an indispensable role in promoting U.S. interests in cyberspace and agree with many of the recommendations in this report. As stated previously, I respectfully defer to Secretary Tillerson on matters about how the State Department can and should be best organized to contribute to U.S. Government efforts in cyberspace.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

Mr. KREBS. The Department of Homeland Security (DHS) works closely with the Department of State, and other interagency partners, as well as foreign governments, regional and international organizations, the private sector and civil society, to foster collaborative efforts to accomplish national and homeland security objectives and to advance an open, interoperable, secure, and reliable cyberspace. At the Under Secretary level, this work is done by the State Department's Under Secretary for Economic Growth, Energy and Environment. NPPD works closely with the State Department's Deputy Assistant Secretary for Cyber and International Communications and Information Policy. DHS defers to the State Department on how best to organize itself to carry out its authorities. Regardless of organizational structure, DHS will continue to work closely with all appropriate offices at the State Department in order to achieve our mission of safeguarding and securing cyberspace. The State Department serves a key role in enabling DHS's international efforts.

31. Senator KAINE. Do you believe it is more or less in U.S. national security interests to gain international agreements on cyber policy compared to when the 2013 Council on Foreign Relations Task Force report titled Defending an Open, Global, Secure, and Resilient Internet report was published?

Mr. RAPUANO. There has been a marked increase in the number and severity of disruptive and damaging cyber activities undertaken by States since the 2013 Council on Foreign Relations report. The May 11, 2017 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure recognizes that the United States, as a highly connected nation, depends on a globally secure and resilient internet. The Executive Order directs the Department of State to develop an engagement strategy for international cooperation in cybersecurity. The Department of Defense is working closely with the Department of State to develop this strategy and I would be happy to discuss this further when the strategy is completed.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

Mr. KREBS. A secure and resilient cyberspace is essential to support critical national functions, enable economic prosperity for the United States, and support American values at home and abroad. Strong cybersecurity is therefore as key element of homeland security. The Department of Homeland Security (DHS) carries

out its cybersecurity mission by leading Federal Government efforts to secure its civilian government information systems; working with the private sector to enhance critical infrastructure cybersecurity and resilience; leveraging the Department's law enforcement authorities to prevent, counter, and disrupt cyber criminals; responding effectively to cyber incidents; and strengthening the security and reliability of the cyber ecosystem through research and development. Each of these DHS cybersecurity missions has an international dimension.

Robust international engagement and collaboration are vital to accomplish the Department's cybersecurity objectives. Poor cybersecurity practices in other countries threaten both federal civilian government information systems and the information systems of non-federal entities, including the owners and operators of critical infrastructure. Insecure devices abroad can be leveraged to directly target networks in the United States. U.S. critical infrastructure is, in particular, increasingly interconnected and dependent on a global infrastructure with widely varied cybersecurity practices.

Other nations and international organizations must therefore be key partners for DHS risk management, network protection, law enforcement, and research and development efforts. Although DHS recognizes that international engagement is essential to achieving its cybersecurity mission, it also understands that this engagement must always be considered in the context of larger national economic and security goals and foreign policy objectives. Accordingly, DHS works closely with the Department of State, other interagency partners, foreign governments, regional and international organizations, the private sector, and civil society, to foster collaborative efforts to accomplish national and homeland security objectives and to advance an open, interoperable, secure, and reliable cyberspace.

SECURING INFORMATION SYSTEMS

32. Senator KAINE. Secretary Rapuano, can you please describe the effectiveness of the SharkSeer program and your plans to bolster it going forward?

Mr. RAPUANO. SharkSeer is highly effective at real-time Active Cyber Defense. It employs advanced near real-time detection, analysis, and mitigation for both known and unknown threats. This includes strong detection and mitigation of zero-day malware and advanced persistent threats (APTs). SharkSeer also includes identification of malicious attachments and links in any email coming from the public internet to DOD users. SharkSeer is already deployed across DOD's unclassified (NIPR), collateral Secret (SIPR), and Top Secret (JWICS) domain boundaries. Leveraging behavioral-based and cloud technologies, SharkSeer provides an integrated solution that stops complex or obfuscated zero-day malware attacks. This includes first order triage of anomalous network traffic and delivery of quick reaction capabilities for critical operational needs. By all accounts, SharkSeer is performing well at desired levels of functionality. The National Security Agency (NSA) and the Defense Information Systems Agency (DISA) are partnering on the development and execution of plans to transfer the SharkSeer Program to DISA under a phased transition plan. Phase I of the transition was successfully achieved on April 20, 2017 with DISA assuming operational C2 and execution of 24/7 SharkSeer perimeter defense operations to include: event triage and malware analysis, countermeasure analysis, mitigation approval, and operational reporting. As the operator of the SharkSeer system, DISA should provide the official evaluation of SharkSeer's effectiveness. Under Phase I of the transition, NSA continues to operate, maintain, and sustain SharkSeer systems and infrastructure. The SharkSeer Program is in sustainment mode pending transfer of the SharkSeer Program to DISA and DISA defining their Perimeter Defense Strategy. Potential future plans for this program include its expansion to the intelligence community, civil, agencies, and mobile device pilots for a comprehensive coordinated defense.

COUNTERING ADVERSARIES IN THE CYBER DOMAIN

33. Senator KAINE. Do any of you participate in war-gaming exercises to better anticipate the ideas and concepts our adversaries may develop for use in the cyber-domain to challenge our national interests both at home and abroad and can you provide some examples that your teams have come up with?

Mr. RAPUANO. The Department of Defense regularly engages in wargaming exercises to improve our ability to anticipate the ideas and concepts our adversaries may develop for use in the cyber-domain to challenge our national interests both at home and abroad. Such games typically involve "red teams" that attempt to emulate adversary actions in the context of the scenario at play. These games occur at all leadership levels of the Department, including within and across combatant commands, Services and components. The rank and make-up of participants are determined by

the wargame's objectives. Such games are typically classified, but one example would be the wargame the Chairman of the Joint Chiefs of Staff, in consultation with the Principal Cyber Advisor, conducted as directed by section 1646 of the National Defense Authorization Act for Fiscal Year 2016. A second example is a wargame conducted at the OSD level in May of 2017 that focused on the cyber resiliency of the GPS Operational Control System.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

Mr. KREBS. Exercises are a core component of the Department of Homeland Security's (DHS) efforts to safeguard and secure cyberspace, a core homeland security mission. DHS conducts or participates in exercises with our interagency partners, including the Department of Defense.

DHS's National Cybersecurity and Communications Integration Center (NCCIC) includes the National Cyber Exercise and Planning Program (NCEPP). The full portfolio of exercises range from small-scale, limited scope, discussion-based exercises to large-scale, internationally scoped, operations-based exercises, such as the biennial Cyber Storm exercise. In addition to Cyber Storm, DHS is a full participant in the annual Cyber Guard exercise. Exercises are designed to assist organizations at all levels, including federal and non-federal entities, in the development and testing of cybersecurity prevention, protection, mitigation, and response capabilities.

PUBLIC-PRIVATE INTERACTION IN CYBER RESPONSE

34. Senator KAINE. Does the Government have a formalized process to evaluate reports generated in the private sector to utilize within government, or is that dependent on personal relationships between public and private officials working in the cyber arena?

Mr. RAPUANO. I respectfully defer to my DHS colleague regarding the details of broader public/private information sharing activities. For DOD, we maintain a robust information-sharing relationship with the private sector and in particular the Defense Industrial Base (DIB) using both formal and informal channels. DOD partners with companies in the DIB through the DIB Cybersecurity (CS) program, sharing both classified and unclassified cyber threat information with industry, including voluntary cyber threat reporting. Additionally, DOD requires defense contractors to report cyber incidents that affect DOD controlled unclassified information, or the contractor's ability to provide operationally critical support. These requirements are implement through Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204–7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting". DOD's partnerships with the private sector combined with regulatory activities help DOD and its private sector partners maintain awareness of the threat environment, track malicious cyber activity relevant to DOD, and inform efforts to harden and protect networks, systems, and information. DOD also benefits from robust information sharing across the Federal Government.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

Mr. KREBS. Collaboration between the public and private sectors is necessary to successfully safeguard and secure cyberspace. Information sharing is a key part of the Department of Homeland Security's (DHS) mission to create shared situational awareness of malicious cyber activity. The National Protection and Programs Directorate's (NPPD) National Cybersecurity and Communications Integration Center (NCCIC) serves as the round the clock operational center that executes the Department's core cybersecurity and communications mission and, as such, facilitates multi-directional information sharing between the Federal Government and the private sector.

There are many formalized processes used to evaluate and share reports generated in the private sector. These processes vary based on the type of report. For instance, the NCCIC has formalized processes for receiving reports of cyber threat indicators, or technical data, which can be shared broadly with network defenders to assist them with their efforts. Through coordinated vulnerability disclosure, the NCCIC regularly receives reports of software vulnerabilities from non-federal entities. By working with partners to identify, validate, mitigate, and disclose these vulnerabilities, DHS leverages formalized processes in its cybersecurity efforts. Finally, the NCCIC has a formalized process for receiving reports of cyber incidents generated by the private sector. DHS and interagency partners follow processes laid out in the National Cyber Incident Response Plan to coordinate our efforts. These are only a few examples of formalized processes. Many others exist to enable successful collaboration between the public and private sectors.

35. Senator KAINE. WannaCry was one of the most effective and timely public private internet attack responses. Was there an institution in place to facilitate this response for us to replicate elsewhere in government, or did this rely on personal relationships?

Mr. RAPUANO. The response to WannaCry followed the U.S. Government's existing framework for incident response, with the Department of Homeland Security functioning as the lead for asset response and the Federal Bureau of Investigation as the lead for threat response. DOD was postured to assess and respond to the incident within DOD and the Defense Industrial Base (for which DOD is the sector specific agency) as well as to support DHS's and the FBI's efforts. In addition, the DOD Cyber Crime Center development and distributed cyber threat products to the DIB.

Mr. Smith did not respond in time for printing. When received, answer will be retained in committee files.

Mr. KREBS. The WannaCry incident is one of many examples where sectors have demonstrated a willingness to work closely with the Department of Homeland Security, a civilian government agency. During WannaCry, the Department of Homeland Security (DHS) led coordination of Federal Government incident response efforts by working with partners in industry, other Federal agencies, state and local governments, and international partners to share information related to WannaCry ransomware. In addition to the regular information sharing prior to the WannaCry ransomware incident, the DHS NCCIC implemented enhanced coordination procedures after learning of the incident in order to coordinate incident response actions across the Federal Government. Through a coordinated federal effort, the NCCIC worked with private sector critical infrastructure owners and operators to assess exposure to the vulnerability exploited by WannaCry ransomware and to share information, including technical data. If requested, NCCIC was also able to provide technical assistance. Relevant private sector outreach included Sector-Specific Agencies for the purposes of engaging their sectors, the information technology sector, the health sector, and small businesses, among others.

During cyber incidents, the Federal Government's roles and responsibilities are guided by statutory authority, Presidential Policy Directive 41, the National Cyber Incident Response Plan, and other presidential direction. When a cyber incident affects a private entity, federal agencies undertake three concurrent lines of effort: threat response, asset response, and intelligence support and related activities. During significant incidents, the Department of Justice, acting through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, is the federal lead agency for threat response activities; the Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, is the federal lead agency for asset response activities; and the Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, is the federal lead agency for intelligence support and related activities. Sector-Specific Agencies for affected critical infrastructure sectors contribute to the interagency response effort by leveraging their well-established relationships within their sector and understanding the potential business or operational impacts on private sector critical infrastructure.

36. Senator KAINE. Mr. Krebs, using WannaCry response as an example, have you found certain sectors or companies less willing to engage in information sharing with civilian government agencies as opposed to Intelligence Community or DOD?

Mr. KREBS. The WannaCry incident is one of many examples where sectors have demonstrated a willingness to work closely with the Department of Homeland Security, a civilian government agency. During WannaCry, the Department of Homeland Security (DHS) led coordination of Federal Government incident response efforts by working with partners in industry, other Federal agencies, state and local governments, and international partners to share information related to WannaCry ransomware. In addition to the regular information sharing prior to the WannaCry ransomware incident, the DHS NCCIC implemented enhanced coordination procedures after learning of the incident in order to coordinate incident response actions across the Federal Government. Through a coordinated federal effort, the NCCIC worked with private sector critical infrastructure owners and operators to assess exposure to the vulnerability exploited by WannaCry ransomware and to share information, including technical data. If requested, NCCIC was also able to provide technical assistance. Relevant private sector outreach included Sector-Specific Agencies for the purposes of engaging their sectors, the information technology sector, the health sector, and small businesses, among others.

During cyber incidents, the Federal Government's roles and responsibilities are guided by statutory authority, Presidential Policy Directive 41, the National Cyber Incident Response Plan, and other presidential direction. When a cyber incident af-

fects a private entity, federal agencies undertake three concurrent lines of effort: threat response, asset response, and intelligence support and related activities. During significant incidents, the Department of Justice, acting through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, is the federal lead agency for threat response activities; the Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, is the federal lead agency for asset response activities; and the Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, is the federal lead agency for intelligence support and related activities. Sector-Specific Agencies for affected critical infrastructure sectors contribute to the interagency response effort by leveraging their well-established relationships within their sector and understanding the potential business or operational impacts on private sector critical infrastructure.

