Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON THE ROLES AND RESPONSIBILITIES FOR DEFENDING THE NATION FROM CYBER ATTACK

Thursday, October 19, 2017

Washington, D.C.

ALDERSON COURT REPORTING
1155 CONNECTICUT AVENUE, N.W.
SUITE 200
WASHINGTON, D.C. 20036
(202) 289-2260
www.aldersonreporting.com

HEARING TO RECEIVE TESTIMONY ON

THE ROLES AND RESPONSIBILITIES FOR DEFENDING

THE NATION FROM CYBER ATTACK

Thursday, October 19, 2017

U.S. Senate

Committee on Armed Services

Washington, D.C.

The committee met, pursuant to notice, at 9:36 a.m. in Room SD-G50, Dirksen Senate Office Building, Hon. John McCain, chairman of the committee, presiding.

Committee Members Present: Senators McCain [presiding], 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 HON. JOHN McCAIN, U.S. SENATOR FROM ARIZONA

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. And 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. And 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. And 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 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. And 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, DHS, and the FBI, 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 organization 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 HON. JACK REED, U.S. SENATOR FROM RHODE ISLAND

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

And 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 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.

And there, indeed, is urgency to our task. Russia attacked our election last year. They similarly attacked multiple European countries, the NATO 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 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 HON. 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 responsibilities, 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 to 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. And 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 subcommittee's interest in these issues. And 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:]

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 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 is absolutely a key and 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 locations across the globe. The FBI also relies upon private sector partnerships leveraging the National Cyber Forensic Training Alliance, InfraGard, 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.

Incident response. 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. And 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. And 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:]

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's 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 Department 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. And 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 for natural disasters that can rise to meet any demand.

And 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. And 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:]

Chairman McCain: Thank you, Mr. Krebs. And 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. And 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 fundamental 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. 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. And 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 -- and I quote -- 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, quote, 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, quote, 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. And 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, quote, 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. And 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. And 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. And we have included in the NDAA 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.

And 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, 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, 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, share information. We are issuing security clearances to a number of election officials, and in a matter of weeks, we are going to establish a sector 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. And 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 responsive of this committee but the legislation that Senator McCain and I are sponsoring for the SEC 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. And 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. And 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.

And 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.

And 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:]

[COMMITTEE INSERT]

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. And 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: And 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. And 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.

And 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. And 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. And 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. And I wish you would consider a subpoena.

Chairman McCain: And 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. And 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.

So, 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. And 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. And 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: And 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 their 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. And 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 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 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.

And 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. And yet, 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. And 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? And 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 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. And I do not mean to interrupt, but I have limited time. And 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 Hewlitt 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 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 -- and I quote -- HP ArcSight software and hardware are so embedded-- end quote -- that it could not consider other competitors'-- quote -- absence and overhaul of the current IT infrastructure. Do you believe that that is what is required? And 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. And 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. And 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 we believe exist between the different agencies responsible for the protection of the cyber systems within our country.

And 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.

And yet, 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. And 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. And 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. And 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. And, Mr. Chairman, if you would not mind.

Here is the key part of this. These attacks are going on now. Talon, Talon 1.0, Talon 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? And are we prepared to take them beyond our borders?

Mr. Rapuano: So, Senator, yes, we do. And 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 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. And 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:]

[COMMITTEE INSERT]

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. And 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. And 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. And 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. And 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. And on US-CERT, 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. And we are moving out aggressively. And 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. And I understand, Mr. Rapuano, that we have plans and capabilities. 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, 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.

And 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. And 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. And that is why I worked with Senators Coons, Fischer, and Gillibrand to introduce bipartisan legislation requiring the DOD to track National Guard cyber capabilities. And, Mr. Smith, you had given a shout-out 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. And 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. And 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 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. And 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:]

[COMMITTEE INSERT]

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.

And, 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. And 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 standards, NIST.

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.

[The information follows:]

[COMMITTEE INSERT]

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. And specifically you identified two malware attacks called BlackEnergy and Havoc. Is that the right pronunciation?

Mr. Krebs: Yes, ma'am.

Senator Hirono: Have specifically targeted industrial control systems. And 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 systems 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: Comp? 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. And 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. And so 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 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. And 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. And 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. And 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. And 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:]

[COMMITTEE INSERT]

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, 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. And, Mr. Smith, you used the term "impose consequences." And 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. And 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: And 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, 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. And I hope in the counsels of the administration that will be an emphasis in your response.

Mr. Rapuano: Yes, I agree, Senator. And 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. And 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. And 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: And 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. And 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? And 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. And 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. And I think that is what we are all going to be waiting for. And 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. And 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. And 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. And 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 was 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 spreadsheet of who and at what level. And 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. And 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. And 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. And 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: And 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. And 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. And 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. And 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. And 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 -- 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: And 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. And 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 can 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, to conduct that assessment itself. 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. And 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. And 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. And 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. And 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? And 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. And 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: And those are in place.

And 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.

And 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. And 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.

And 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. And 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. And 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?

And 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. And 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: And so the question is -- and Senator Peters raised it -- what is, for want of a better term, the trigger? And 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. And 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, followed 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.

And 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.

And 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. And 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 hearing was adjourned.]