[H.A.S.C. No. 114–52]

IMPLEMENTING THE DEPARTMENT OF DEFENSE CYBER STRATEGY

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

HEARING HELD
SEPTEMBER 30, 2015

U.S. GOVERNMENT PUBLISHING OFFICE
97–198 WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ARMED SERVICES

ONE HUNDRED FOURTEENTH CONGRESS

WILLIAM M. "MAC" THORNBERRY, Texas, *Chairman*

WALTER B. JONES, North Carolina
J. RANDY FORBES, Virginia
JEFF MILLER, Florida
JOE WILSON, South Carolina
FRANK A. LOBIONDO, New Jersey
ROB BISHOP, Utah
MICHAEL R. TURNER, Ohio
JOHN KLINE, Minnesota
MIKE ROGERS, Alabama
TRENT FRANKS, Arizona
BILL SHUSTER, Pennsylvania
K. MICHAEL CONAWAY, Texas
DOUG LAMBORN, Colorado
ROBERT J. WITTMAN, Virginia
DUNCAN HUNTER, California
JOHN FLEMING, Louisiana
MIKE COFFMAN, Colorado
CHRISTOPHER P. GIBSON, New York
VICKY HARTZLER, Missouri
JOSEPH J. HECK, Nevada
AUSTIN SCOTT, Georgia
MO BROOKS, Alabama
RICHARD B. NUGENT, Florida
PAUL COOK, California
JIM BRIDENSTINE, Oklahoma
BRAD R. WENSTRUP, Ohio
JACKIE WALORSKI, Indiana
BRADLEY BYRNE, Alabama
SAM GRAVES, Missouri
RYAN K. ZINKE, Montana
ELISE M. STEFANIK, New York
MARTHA MCSALLY, Arizona
STEPHEN KNIGHT, California
THOMAS MACARTHUR, New Jersey
STEVE RUSSELL, Oklahoma

ADAM SMITH, Washington
LORETTA SANCHEZ, California
ROBERT A. BRADY, Pennsylvania
SUSAN A. DAVIS, California
JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JIM COOPER, Tennessee
MADELEINE Z. BORDALLO, Guam
JOE COURTNEY, Connecticut
NIKI TSONGAS, Massachusetts
JOHN GARAMENDI, California
HENRY C. "HANK" JOHNSON, JR., Georgia
JACKIE SPEIER, California
JOAQUIN CASTRO, Texas
TAMMY DUCKWORTH, Illinois
SCOTT H. PETERS, California
MARC A. VEASEY, Texas
TULSI GABBARD, Hawaii
TIMOTHY J. WALZ, Minnesota
BETO O'ROURKE, Texas
DONALD NORCROSS, New Jersey
RUBEN GALLEGO, Arizona
MARK TAKAI, Hawaii
GWEN GRAHAM, Florida
BRAD ASHFORD, Nebraska
SETH MOULTON, Massachusetts
PETE AGUILAR, California

ROBERT L. SIMMONS II, *Staff Director*
KEVIN GATES, *Professional Staff Member*
LINDSAY KAVANAUGH, *Professional Staff Member*
NEVE SCHADLER, *Clerk*

CONTENTS

IMPLEMENTING THE DEPARTMENT OF DEFENSE CYBER STRATEGY

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
Washington, DC, Wednesday, September 30, 2015.

The committee met, pursuant to call, at 10:00 a.m., in room 2118, Rayburn House Office Building, Hon. William M. "Mac" Thornberry (chairman of the committee) presiding.

OPENING STATEMENT OF HON. WILLIAM M. "MAC" THORNBERRY, A REPRESENTATIVE FROM TEXAS, CHAIRMAN, COMMITTEE ON ARMED SERVICES

The CHAIRMAN. The committee will come to order. Let me welcome our witnesses and guests for our second hearing this week at the full committee level on cybersecurity. We are very pleased to have a distinguished panel of witnesses to help us with this challenging area.

For those members who were able to participate in our hearing yesterday, we heard from the private sector and from academia, think tanks, about some of the challenges that we face in cyber. For example, questions such as: What is the role of the military in defending private infrastructure? Should private industry be able to hack back against those who may try to steal their intellectual property? What does "deterrence" mean when it comes to cyber?

A number of difficult questions that we talked about some, but we will continue to pursue that line today. Cyber, as many people say, is a new domain of warfare, and so what that means for the Department of Defense [DOD], what that means for our country's national security is very much at or near the top of the agenda for all of us who are involved in national security.

Before I turn to our distinguished panel of witnesses, I will yield to the distinguished ranking member for any comments he would like to make about today's hearing.

STATEMENT OF HON. ADAM SMITH, A REPRESENTATIVE FROM WASHINGTON, RANKING MEMBER, COMMITTEE ON ARMED SERVICES

Mr. SMITH. Thank you, Mr. Chairman. I appreciate you holding this hearing and the one yesterday.

Our outside experts sort of basically said that the strategy is sound. It is the implementation that is key. And, obviously, this is a very difficult area of public policy. It is constantly evolving. The threat changes every single day. We have to prepare to meet that threat.

I think a lot of it is, you know, having the right personnel, having very, very smart people who understand technology, and obviously, we have to compete against private industry as we try to bring those folks in. So that is definitely a challenge.

Coordination is also a challenge. There are so many different pieces of the Department of Defense: Who is in charge of cyber strategy, and how is it being implemented DOD-wide because, as we all know, the big problem with cyber is the classic single point of failure. You can get absolutely everything right except for one thing and have a disaster. How do we comprehensively make sure that we are taking into account every single one of those points of failure? That is not easy to do.

And then some of the questions that the chairman raised about, you know, when is offensive cyberattacks okay? What are the rules of the road? And I think that that is a real challenge as we deal with China, as we deal with Russia, as we deal with Iran and others. What are the red lines, and how do we respond if someone crosses those red lines?

I know that the agreement that was reached with China on this is unsatisfactory to many. It is unsatisfactory to me. It has a long way to go, but I think we need to have those types of conversations, certainly with Russia and China, so that we better understand what the rules of the road are so that we can get to the point where we don't, you know, stumble into something greater than we had expected.

But I know cyber policy isn't easy, but I look forward to hearing from Deputy Secretary Work and our other witnesses on how we can get our arms around it and then, also, of course, you know, what the legislative branch can do to make it easier for you to implement those policies.

So thank you, Mr. Chairman. I yield back.

The CHAIRMAN. Thank you.

Again, I want to thank our distinguished witnesses for being here. We are very pleased to have the Honorable Robert Work, Deputy Secretary of Defense; Admiral Michael Rogers, the Commander of USCYBERCOM [U.S. Cyber Command]; and Mr. Terry Halvorsen, the Chief Information Officer [CIO] for the Department of Defense.

Without objection, your full written statements will be made part of the record. Thank you for submitting those.

And, Mr. Secretary, we will turn the floor over to you for any comments you would like to make.

STATEMENT OF HON. ROBERT O. WORK, DEPUTY SECRETARY OF DEFENSE; ACCOMPANIED BY TERRY HALVORSEN, CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE

Secretary WORK. Thank you, Chairman Thornberry, Ranking Member Smith, distinguished members of the committee.

Thank you for inviting us here this morning to discuss the Department of Defense efforts in cyberspace. As both the chairman and the ranking member said, this is an extremely important issue that we grapple with every day. And so we welcome these types of meetings to discuss the policy issues.

As you know, cyber intrusions and attacks by both state and nonstate actors have increased dramatically in recent years. And particularly troubling to us, as the Department of Defense and as a nation, are the increased frequency in scale of state-sponsored cyber actors breaching U.S. Government and business networks. These adversaries continually adapt and evolve in response to our cyber countermeasures. They threaten our networks and systems of the Department of Defense, our Nation's critical infrastructure, and the U.S.' companies and interests globally.

The recent spate of cyber events that have been in the press, the intrusions into OPM [Office of Personnel Management], the Sony, and the Joint Staff networks by three separate state actors is not just espionage of convenience, but a threat to our national security.

As one of our responses to this growing threat, the Department recently released its 2015 DOD Cyber Strategy, which will guide the development of our cyber forces and strengthen our cybersecurity and cyber deterrence posture.

We have three core cyber missions, as defined in our strategy. First and foremost—and this is what Secretary Carter has made a clear number one priority first—is to defend DOD network systems and information. That is job number one. Second, we help defend the Nation against cyber events of significant consequence. And third, we provide cyber support to operational and contingency plans in support of our combatant commanders. And in this regard, U.S. Cyber Command may be directed to conduct cyber operations in coordination with other U.S. Government agencies, as appropriate, to deter and defeat strategic threats in that domain.

Now, my submitted statement contains additional detail on how we are moving to achieve these goals, but I would like to highlight a particular focus, which is bolstering our cyber deterrence. This was a big issue yesterday in the Senate Armed Services Committee.

I want to acknowledge to all of you upfront that in terms of deterrence, we are not where we need to be as a nation or as a Department. We do believe that there are some things the Department is doing that are working, but we have to improve in this area, and that is why we have revised our cyber strategy.

Deterrence is a function of perception. First and foremost, it works by convincing a potential adversary that the costs of conducting the attack far outweigh any potential benefits that they might gain from it. The three main pillars of our strategy are denial, resilience, and cost imposition.

When we talk about denial, denial means preventing a cyber adversary from achieving their objectives.

Resilience is ensuring that our systems will continue to perform their essential military tasks, even in a cyber-contested environment or while under attack.

And cost imposition is our ability to make sure cyber adversaries pay a much higher price for the malicious activities than they had hoped for.

I would like to just dive down deep into these three kinds of pillars very, very quickly. To deny an attacker the ability to adversely impact our military missions, first and foremost, we have to defend our own information networks and data systems. Now, we have

made a lot of investments in this regard, and we believe they are starting to bear fruit, but technical upgrades, this is not just about technical upgrades. Because nearly all successful network exploitations up to this point can be traced to a single or multiple human errors, raising the overall level of individual cybersecurity awareness and performance throughout the Department is absolutely paramount. So we are working to transform our DOD cybersecurity culture for the long term by improving human performance and accountability within our systems.

As part of this effort, we just recently published a cybersecurity discipline implementation plan and a scorecard, the first of its kind. The first time it was implemented was in August of this year. These, we believe, are going to be critical to our strategic goal of defending the networks and securing our data and mitigating risks to our missions. The new scorecard system is reported to the Secretary and me on a monthly basis, and it will hold commanders accountable for hardening and protecting their end points and critical systems, and directs compliance with our overall policy.

Denial also means defending the Nation against cyber events of significant consequence. The President has directed DOD, working in partnership with other agencies, to be prepared to blunt and stop the most dangerous cyber events against our Nation and its infrastructure. There may be times where the President or Secretary of Defense directs DOD and others to conduct a defensive cyber operation to stop a cyberattack from impacting our national interests. And so that means to us we have to build the capabilities to prevent or stop a potential cyberattack from achieving its effect.

This is an extremely challenging mission. It requires high-end teams and capabilities, and we are building our Cyber Mission Force and deepening our partnerships with law enforcement in the Intelligence Community, and we can talk about that in questioning.

A second principle of deterrence is improving our resiliency by reducing the ability of our adversaries to attack us through cyberspace and protecting our ability to continue to execute missions even while in a degraded cyber environment.

Our adversaries unquestionably view DOD cyber dependency as a potential wartime vulnerability. Therefore, we have to have the ability to fight through these cyberattacks as a mission-critical function. That means normalizing cybersecurity as part of our mission assurance efforts, building redundancy into our systems whenever they are vulnerable, and training constantly to operate in a contested cyber environment.

Our adversaries have to see over time that cyberattacks will not provide them a significant operational advantage, and that will be one of the key aspects of deterrence.

The third and final aspect is having the demonstrated capability to respond with cyber or noncyber means to impose costs on a potential adversary. The administration has made clear that the United States will respond in a time, manner, and place of our choosing, and it has developed cyber options to hold aggressors at risk, if required.

Successfully executing our missions in cyberspace requires a whole-of-government and whole-of-nation approach. This is a much,

much, much more difficult problem than the debates we had over nuclear weapons in the 1950s. For that reason, DOD continues to work with our partners and other Federal departments and agencies, the private sector, and our partners around the world to address the shared challenges we face.

Secretary Carter, I think you know, has placed a particular emphasis on partnering with the private sector. We know we do not have all the right answers, and our working with industry will be very, very critical to make sure we have both the cutting edge of technology as well as best practices and procedures.

Finally, our relationship with Congress is absolutely critical. We very, very much appreciate the support for DOD cyber activities both last year and this year, as we understand, in the 2016 National Defense Authorization Act [NDAA]. I encourage continued efforts to pass legislation on cybersecurity information sharing, on data breach notification, and law enforcement provisions related to cybersecurity, which were included in the President's legislative proposal submitted earlier this year.

The American people expect us to defend against cyber threats of significant consequence. The Department looks forward to working with this committee and Congress to ensure we continue to take every step possible to confront the substantial cybersecurity risk we face.

Thank you for inviting us here today, Mr. Chairman, and the attention you are giving this urgent matter. I look forward to all of your questions.

[The prepared statement of Secretary Work can be found in the Appendix on page 49.]

The CHAIRMAN. Thank you, sir.

Admiral Rogers, thanks for being here. You are recognized.

STATEMENT OF ADM MICHAEL S. ROGERS, USN, COMMANDER, U.S. CYBER COMMAND

Admiral ROGERS. Sir, thank you. Chairman Thornberry, Ranking Member Smith, and distinguished members of the committee, I am honored to appear before you today and before the American people to explain how we are implementing the Department of Defense Cyber Strategy. I thank you for convening this forum and for your efforts in this important area. I am equally pleased to be sitting alongside today Deputy Secretary of Defense Work and the DOD CIO Terry Halvorsen.

It gives me great pride today to highlight the accomplishments of the uniform and civilian personnel of U.S. Cyber Command and its components. I am both grateful for and humbled by the opportunity that I have been given to lead this cyber team. U.S. Cyber Command and its subordinate elements have been given a responsibility to direct, operate, and secure the Department's systems and networks, which are fundamental to the execution of all of DOD's missions. The Department and the Nation rely on us to build ready cyber forces and to be prepared to employ them when significant cyber events against the Nation require DOD support.

We are expected to work closely with other combatant commanders to integrate cyber operations into their broader military

missions. Policy makers and commanders alike look to us for cyber options in all phases of operations.

Our military is in constant contact with agile learning adversaries in cyberspace, adversaries that have shown the capacity and the willingness to hit soft targets in the U.S. The demand for our cyber forces continues to outstrip supply as we bring more capability online, but we continue to rapidly mature based on real world experiences and the hard work of the men and women of U.S. Cyber Command and our service cyber components.

The Secretary of Defense and the Department of Defense Cyber Strategy direct us to intensify our efforts to defend the United States and its interests in our digital age. It is my intent that we move forward quickly with our partners to build our military capabilities, and I have provided this guidance in a recently released Commander's Vision and Guidance for U.S. Cyber Command.

In line with that guidance, we are building and employing the Cyber Mission Forces. We are conducting exercises with our interagency and private sector partners to inform whole-of-nation responses to crises in cyberspace, and we are supporting DHS [Department of Homeland Security] and FBI [Federal Bureau of Investigation], when directed, to defend the Nation's critical infrastructure from cyber incidents. We support operational commanders around the world every day.

The bottom line is we are being challenged as never before to defend our Nation's interests and values in cyberspace against states, groups, and individuals that are using increasingly sophisticated capabilities to conduct cyber coercion, cyber aggression, and cyber exploitation. The targets of their efforts extend well beyond government and into privately owned businesses and personally identifiable information.

I welcome this opportunity to elaborate on the progress we have made to date and where we should be focussing going forward to ensure that we continue to stay ahead and deter threats to secure our digital networks and our combat systems, to ensure our ability to execute the Department's missions.

With that, I look forward to your questions, and thank you again for taking the time today to spend on this important topic.

[The prepared statement of Admiral Rogers can be found in the Appendix on page 58.]

The CHAIRMAN. Thank you, sir.

And, Mr. Halvorsen, I understand you do not have a prepared statement but are available to answer questions. Is that correct?

Mr. HALVORSEN. That is correct, sir.

The CHAIRMAN. Great. Thank you for being here, sir. I appreciate it.

Admiral Rogers, yesterday, one of our witnesses made the point that in any challenge in warfare, what counts is the net assessment. In other words, we can talk about what we are doing, but what really counts is what the results of that versus what the adversaries are doing. And so just at the very highest level, as you look at cyber as a domain of warfare, how would you describe the net assessment, where we are today and where those trends are taking us? Are we in a good direction to reduce the vulnerabilities and have the capabilities we need? Are the adversaries moving

faster than we are? How would you describe that kind of net-net in cyber today?

Admiral ROGERS. So this is a mission set where I think we have to acknowledge we have at least one peer competitor in the form of the Russians when I look at their level of capability, when I look at their activity. Then we have a set of other nation-states we pay great attention to who I am watching increase their level of investment, increase their capacity, and their capability. The Chinese are probably the ones that get the most attention, if you will, but they are not alone by any stretch of the imagination.

The challenge for us, in many ways, is we are attempting to overcome literally decades of investment with a very different attitude, where redundancy, resiliency, and defenseability in terms of our systems—whether they be our networks, whether they be the combat systems and the platforms that we count on to execute our missions—defenseability, redundancy, and resiliency were, until only recently, they were never core design characteristics. They tended to be something that we thought of after we focused on efficiency, cost, speed.

And so we find ourselves trying to overcome literally decades of investment, of sunk capital costs, if you will, if I was a business. I think we have got a good strategy, a good vision for where we need to go. The challenge always is you are never as fast as you want to be. So as a commander, the argument I have made with my teams is: So this is all about prioritization, Team. We have got to step back and assess where do we think the greatest vulnerabilities lie, where do we think our opponents are most interested in attempting to generate effects against us, and how do we forestall their ability to do that in broad terms.

The CHAIRMAN. So, to summarize, we are getting better but not better fast enough.

Admiral ROGERS. I think that is a fair——

Secretary WORK. Mr. Chairman, if I could add something to this on the net assessment side.

The CHAIRMAN. Yes, sir.

Secretary WORK. All of the adversaries that we face are generally, in this regard, are authoritarian powers. We are the most open nation on the Earth. It is a tremendous competitive advantage, but it provides—we are much more open on our Internet than our adversaries are in their own countries. That makes us inherently more vulnerable. The number of attack surfaces that we have to defend against are very, very much larger. So in terms of net assessment, that is one of the things that are challenging us and we are trying to sort through.

The CHAIRMAN. Okay. Thank you.

Mr. Secretary, I want to ask you, on the three core missions you laid out, number two is defend the Nation against significant cyberattacks. As you know, there has been considerable conversation about what that means. So if I am a company under cyberattack, when is the government going to come help defend me? And I realize you probably can't put a dollar threshold or something very specific on what that means, a significant cyber event, but can you help clarify for us, when the Department of Defense becomes en-

gaged in defending the country and what that means, significant cyber event?

Secretary WORK. Well, those were the—we call it a cyber event or activity of significant consequence.

The CHAIRMAN. I am sorry, Mr. Secretary, is your microphone on?

Secretary WORK. I am sorry, sir. You are exactly right. We are obligated to defend the Nation against cyberattacks or cyber activities of significant consequence, and that is not a purely defined term. Each attack would be looked at. So, for example: Did the attack result in any death? Injury? Significant destruction was associated with it? Was it an act of espionage? Was it an act of cybercrime? In other words, was it a nonstate actor who is trying to get a PII [personally identifiable information]? But a significant consequence would be things which would go against our national critical infrastructure, and this would be decided primarily with the Department of Homeland Security, which would have the lead on attacks within the United States on critical infrastructure, and we would then work through with the policies to make an appropriate response.

Admiral Rogers works this constantly, so I think he would be very well placed to answer this question, too.

Admiral ROGERS. I would agree completely with the Secretary.

It explains why the response to Sony, for example, is very different than the response to OPM. We try to look at things in a case-by-case basis given a specific set of facts, and we are clearly still working our way through some of these broader definitions. I don't think there is any doubt about that.

The CHAIRMAN. Well, I appreciate it. I think other members may want to follow up.

I mean, you look at OPM and huge consequences for our national security. I presume if you had seen it occurring, then there would have been action taken to prevent it, but it is large consequences, even for the theft of information that did not result in death, we trust.

Mr. Smith.

Mr. SMITH. Thank you.

And I know you can't talk about this in an open setting in terms of what our response has been to some of these cyberattacks, but can I ask if, you know, you feel that response has been effective? Has it deterred more attacks? At this point, how comfortable are you that our responses to—and again, there are, as you have laid out, levels of cyberattacks. When you pass a certain level, then, you know, we feel like a response is appropriate, have those responses been at all effective in your view at this point? And how would you define effectiveness?

Secretary WORK. I would say at this point we don't believe that our deterrence policy has been effective up to this point or as effective as it should be, and that is why we want to strengthen it. As we talked, one of the problems is attribution. So the first thing is, where did the attack come from, a geographical location? Then who was the actor who the attack came from? And then did the state control the actor, or was the actor operating independently?

So that will tell you whether it is a law enforcement response, whether it should be economic sanctions, whether it should be offensive or defensive cyber operations. And I believe what we have to do is have a very strong policy on cost imposition, which we are working towards and we have announced, and then we have to prove that through our actions. So I would say that we are not where we would want to be in terms of deterrence right now.

Mr. SMITH. And following up on that, how effective are you at figuring out where the attack came from? Now, I understand there is the final piece of that is the one that is really most difficult because even if you were to determine who the actor was, was that person acting on their own or acting at the behest of a government? But how effective are you at when an attack comes in saying, all right, tracing it back and saying, that is the person who did it?

Admiral ROGERS. We continue to gain increased insight and knowledge in that area. If you look, for example, using Sony as an illustrative example, we were very quickly able to determine the nation-state and the specific actor within the nation-state. I think that is one reason, again, why you saw, you know, a policy response that was relatively quick. We were able to provide policymakers with a high level of confidence as to who did it, how they did it. It really varies. Though I will say we are watching actors around the world as they realize that we are gaining increased capability in our ability to attribute cyber activity, specific nation-states, specific groups.

It is interesting watching them now attempt to obscure that, create different relationships, use different processes, so this is one, as was indicated in the opening, the dynamics here just change so quickly. It is the nature of this. I don't see that fundamental changing any time soon.

Mr. SMITH. Right.

Secretary WORK. One of the problems is we have a very strong policy that we will respond in a place and a time and a manner of our own choosing, and the problem with this is it is not like it can happen sometimes very, very quickly. First, we have to go through the attribution phase. Then we have to determine: Was it cybercrime? Was it an independent actor? Was the actor responding in charge of the state? And what are the appropriate responses? That might a law enforcement measure. It might be economic sanctions. It might be offensive or defensive cyber operations. It could be military operations, depending on the damage or threat of the attack to our Nation.

So this is much, much different than nuclear deterrence where you can attribute the attack immediately, generally, and you have specific response options already ready. In this case, it is a much more whole-of-government approach that takes more time.

Mr. SMITH. Understood.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Mr. Jones.

Mr. JONES. Mr. Chairman, thank you very much.

You know, this is the new world we all live in. We all know that. It is kind of interesting—I am getting to a question in just a moment—but I bank with the credit union here in Washington. So,

last Saturday, I started calling 24-hour banking to find out what was in my account. As of today, they are not online.

Well, I am certainly not saying that is a cyberspace invasion of anything, but it is just the complexities of the world we are living in now. So when I hear your testimony, I want to first say thank you for who you are and what you are doing.

My next question would be, at this point, knowing that we are constantly here in Washington worried about a shutdown, worried about the debt growing, I will never forget—I have had reason to call Admiral Mullen recently—of course, he is retired—the former chairman—I have great respect for him—on a totally different subject. And I have used many times back in my district, the Third District of North Carolina, the home of Camp Lejeune, Cherry Point, I have used many times what he said when he was chairman: The biggest threat to our military is the debt of our Nation.

What I would like to note, as you move forward to give us the very best protection that you can, what type of financial commitment should the taxpayers and the Congress understand that we need to make to ensure that we have got the best protection?

Secretary WORK. I believe we have been very clear, sir, that the President's request, the PB16 [President's budget 2016] request, we believe, is the absolute minimum needed to provide the national security necessary for the United States.

I would just like to say, I was talking with the chairman just before this, and we are very, very thankful—or we hope—that we will avoid a shutdown. This would be extremely disruptive. I think Admiral Rogers can tell you: the last time we went through a shutdown, it set us back 6 months in terms of preparing our Cyber Mission Force. So we believe the PB16 level is the absolute minimum.

I would also like to say that, you know, in the last 6 years, we have been under a CR [continuing resolution] for 2 years of the 6 years, and each of the first quarters of the fiscal year, we have been under a CR for about 93 percent of the time. In essence, we are operating in a 9-month fiscal year. There is no COO [chief operations officer] in the United States who could operate under this type of uncertainty, and we hope that the CR will be handled or will be resolved as quickly as possible.

So I very much thank the question, sir. This is an important thing. I hope that we will be able to resolve our differences on the budget level and provide for the national security.

Admiral ROGERS. If I could.

Mr. JONES. Excuse me.

Go ahead, Admiral, please.

Admiral ROGERS. The only other comment I would make is, and I think it goes to the point you are trying to make: There shouldn't be any doubt in anyone's mind that there is a cost component to all of this, that, as a Department, we try to prioritize that because we clearly realize there are many competing requirements and resources are tight for the Nation, and we certainly understand that. But there just shouldn't be any doubt that there is a cost component to that. And that cost may change over time, but I don't think it is going to get cheaper for us, at least in the near term, not with the level of activity that you see out there every day.

Secretary WORK. Congressman Jones, I will tell you that, regardless of level of our budget, Secretary Carter has made it clear that cyber defense and cybersecurity is going to be at the very, very top of our priority list. So whatever budget we receive, cyber will receive the attention that we believe it deserves.

Mr. JONES. Well, I believe that the shutdown will probably be avoided, which you know, not getting into the politics of that, but I think it probably will be. And I think you all have done a great job. I think the American people, like me—I am not talking about my colleagues—have really understood that this threat of cyberspace warfare in any form is probably at the foremost, as you said, Admiral, will grow and the threat will become more and more. So I thank you gentlemen for being here today and your testimony.

And I yield back the balance of my time.

The CHAIRMAN. Thank you.

Mrs. Davis.

Mrs. DAVIS. Thank you, Mr. Chairman.

And thank you to all of you for being here. And as you know, we heard from outside groups, the private sector, yesterday, and I think you spoke, certainly, Mr. Secretary, to the importance of that partnership. One of the questions I basically asked them was, you know, what hampers that relationship? What hampers moving forward? And they spoke of the regulatory burden that is placed on companies wishing to work and partner with the DOD, and particularly for newer companies who don't have a history of working with the government.

And so I am wondering how can we make that process easier? Do you think that is a appropriate analysis or response? You may feel that you have done everything you can to assist in that way, but obviously, there is a different response.

The other issue is really whether or not we are kind of losing out on working with some of the best minds in the business because we just make it so difficult for them to work with the Department of Defense.

Secretary WORK. Congresswoman, I would ask Terry Halvorsen, our CIO, who works extensively with the private sector, to answer your question. I think he is the best to do that.

Mr. HALVORSEN. Thank you, sir.

I think there is absolutely some truth that we have got to get better at bringing in particularly newer companies. I think, first, you have to understand, if DOD was a Fortune 500 company, we are Fortune 1. We are very big. That in itself causes us some difficulty with companies that do not have experience with us.

So in the last year, some of the things that we have done to make that better, we have reached out, as many of you have seen, to Silicon Valley. We are holding different events to make industry clearer. One of the things that we did last year, which I thought was one of the bigger breakthroughs, you probably will ask me a little bit later about Cloud. One of things we did to make Cloud easier for people to play and easier for industry to get in, we wrote our new Cloud policy completely with industry. First time we have done that. They actually—we convened them, we brought them in from the beginning. We had leading industry providers—I think

Amazon—on the panel to write that. We have gotten very good reviews from that. We have got to continue to do that.

This year we are going to bring some industry players into the DOD CIO staff and some of the other service CIO staffs. We will actually do exchange with the industry. Some of that will be focused on some of the new industries so that we learn how they need to respond and how we need to respond.

So we have to do better. I think we are doing better in that area, and I think you will see more results in the next 6, 7 months coming down that we will be able to concretely show you what we have done to improve that relationship.

Mrs. DAVIS. Yeah, that is good to hear. I think we have to continue to push and, obviously, ask them how that is working. I guess we also would agree that in the procurement areas, again, maybe there are some better ways of doing it. And everybody talks about it, but sometimes it feels like nothing is getting done.

So I wanted to ask you as well in terms of the hiring as well because in personnel areas, we know that we are not as adaptive in hiring as, obviously, as the private sector is. What are we doing to make sure that in the field of cybersecurity that we are able to push through nominations to positions so that they don't have to wait so long that they go ahead and take those jobs in the private sector?

Mr. HALVORSEN. Two things, and first of all, let me thank all of you. You did pass good legislation that gave Mike Rogers and I some more authority to directly hire people without having some of the normal rules and regulations that we have to follow so we could compete. I know there is some work on some additional. We would appreciate that.

I think one fact we just have to understand: we are not going to pay exactly as much as industry in the cybersecurity area and some other areas. One of the things we have going for us: we have a pretty exciting mission. So when I talk to—and I spend a lot of time talking to people who want to come to work for DOD. We are trying to attract them, and we have been able to pull some people in even the last year into my staff. As long as we can get them in fast and offer them the right wage, which the new authority gives us, I think we will be able to continue in the right—they want to work this mission. And your legislation that recently passed has really helped us with that. Thank you.

Admiral ROGERS. If I could just add, this is one area where I suspect over time we may in fact end up coming back to you as our experience tells us, are there things we could be doing differently? Are there challenges here we need your help in overcoming? Because I always remind people, look, while we spend a lot of time focused on technology, don't ever underestimate, at its heart, this is an enterprise powered by men and women. And they are our advantage, and that is where we need to make sure we are getting really good talent.

To date, I would argue, at the mission force level, the execution piece for us, we have been able to exceed our expectations both in terms of the ability to bring in quality people, as well as retaining them.

Mrs. DAVIS. Perhaps some chart showing the differences as a result of some of these changes would be really helpful in understanding what the impact has really been. Thank you.

The CHAIRMAN. Thank you.

And as I mentioned earlier, we stand ready to work with you all on those authorities as we assess how they are doing. That is very important.

Mr. Forbes.

Mr. FORBES. Thank you, Mr. Chairman.

And I reiterate what Mr. Jones said in thanking each of you for what you do for our country and for being here today.

Mr. Secretary, you probably think strategically and analytically on national defense issues as well as anybody we have in government today, and we appreciate and respect your opinions as you come before this committee.

I would like to follow up on some questions that the chairman offered specifically related to net assessment, and one of the things that I just want to ask, as you are aware, some of the best strategy we have developed over the years have been informed and supported by the practice of net assessment. Has DOD done any net assessments of the cyber domain at this particular point in time?

Secretary WORK. Well, as you know, sir, we just had a leadership change in the Office of Net Assessment [ONA]. It reflects Secretary Carter's very strong support of that office in providing independent assessments to him and I. Jim Baker, who is the new director, has just gotten in and is going to come back in. Cybersecurity and cyber is at the very top of our list, but there are many, many other strategic challenges, as you know.

This one is going to be one that I believe ONA is going to help us on, but I know of nothing at this point as far as an ongoing assessment, but we expect to be able to start asking Mr. Baker.

Mr. FORBES. And that is not a criticism; it is an encouragement. As the chairman talks about net assessment, if we haven't done a net assessment of that, it is kind of difficult to know where we are. So I think we would just encourage, perhaps, the Department, if it can, to do what it can to have that net assessment done, and because I do think it helps us in determining what our strategies are going to be.

The second part of that is I know you have worked very, very hard and very, very well on a third offset strategy. Do you expect that cyber will be a part of that third offset strategy?

Secretary WORK. Absolutely. We assume that the future will be an extremely highly contested cyber and electronic warfare environment. So no matter what strategy we have, that kind of is the underlying baseline that we assume we must be able to contend with.

There are a lot of questions on whether or not—many people say, well, if you go to a more network force, are you going to be able to have the certainty that you will have the networks when you need them? Will you have the confidence? So it will be absolutely critical to the third offset, yes.

Mr. FORBES. And, once again, just an encouragement, the net assessment often really helps us inform what we are doing, that having that net assessment done would be, I think, very helpful.

Admiral Rogers, do you think we need to leverage a wider range of tools, like sanctions, or diplomacy, criminal proceedings, to deter cyberattacks with the threat of punishment? And can you tell us a little bit more about what options you think would be most effective at imposing costs upon perpetrators?

Chairman Wilson and I, for example, have introduced legislation calling for targeted economic sanctions, but I am not asking you to address that bill——

Admiral ROGERS. Right.

Mr. FORBES. But what else? What do we have? What else do we need, in your opinion?

Admiral ROGERS. That has been part of our strategy to date, that just because someone comes at us in a cyber domain doesn't mean the response has to be primarily or purely back in that same arena, if you will.

You see that reflected in the response to the attack on Sony, for example, where we publicly acknowledged the event. We publicly attributed the event. And we talked about an initial set of actions we are going to take in response. In this case, it was economic sanctions. And then the President also talked about and we will take additional action if that is required, we believe, at the time and place of our choosing.

We have used the legal framework within the last year where we have indicted individuals of foreign states, individual actors, we have indicted them. We have done the economic piece. There is a broad range of options that are ongoing with law enforcement, what the FBI, for example, does every day today.

Mr. FORBES. I hate to interrupt you, but I only have——

Admiral ROGERS. Go ahead.

Mr. FORBES [continuing]. 50 seconds, and I would just like to ask you this. Secretary Work said that we have not been as effective up to date as we would like to be. Fair. Again, no criticism, just an observation.

What do you attribute that to? Is it our lack of willingness to use the tools we have, or does this committee need to help you get more tools? What would you say is your assessment of how we make that more effective?

Admiral ROGERS. I mean, I think clearly there is a broad range of tools available to the Nation to include cyber options. One of my particular responsibilities is to be able to generate cyber options so that the Secretary has options to tee up. We are in the relatively early stages of that journey, but we are on that journey, and we have developed some levels of capabilities already. I am not going to get into specifics.

I think the biggest challenge in some ways is just time. I mean, we are in the very early stages of this, and if you look at, for example——

Mr. FORBES. Speaking of time, my time is up, but if you don't mind, we would submit some questions on the record.

Admiral ROGERS. Okay.

Mr. FORBES. And maybe you can respond back.

Admiral ROGERS. Be glad to.

Mr. FORBES. With that, Mr. Chairman, thank you.

And, with that, I yield back.

The CHAIRMAN. Thank you.

The gentleman from Rhode Island, who has been a leader in this area for some time, is recognized for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank you and the ranking member, as well as Chairman Wilson, for the time and attention that you and the committee have put into focussing on cyber.

And, Mr. Secretary, and Admiral, and Mr. Halvorsen, we thank you for your testimony here today.

I think that the discussion we have been having on imposing costs on our enemies and adversaries is critically important, and I am not going to ask a question on this today, but I will say that I know that the committee and certainly I am going to pay a lot of attention on this. We are looking for specifics about what those costs being imposed on our enemies and adversaries will be.

I know the American people are looking for answers on this because right now, up until now, our enemies, adversaries have been eating our lunch for a long time, especially when it comes to cyber espionage, especially when it comes to things like defense contractors over the years.

I know we have gotten better, and we have had the DIB [defense industrial base] pilot in place now, and the follow-on program that has done a better job of defending our defense contractors and the like, but imposing costs on our enemies and adversaries has to be an important part of the equation, and they have to know what it is. I know some of our responses may be classified, but others we need to make public so that our enemies know, our adversaries know that they can't operate with impunity, which is what really is happening right now. It is like the Wild West out there, and they are on the better side of the equation. We have got to flip that so we have better outcomes on our side.

So let me just turn to another topic. Do you believe—and Mr. Secretary, we will start with you—that there is an effective accountability mechanism in place for reported cybersecurity breaches at defense contractors? And could you describe to us the process by which contractors are held accountable?

Secretary WORK. Congressman, I do believe we have an effective means. We are getting better. We have established our own cyber scorecard. This has been one of CIO Halvorsen's top jobs, so I would ask him to answer the question with more specifics.

Mr. HALVORSEN. Thank you, sir. As you mentioned, sir, we actually have improved the DIB process, which brings and gives the companies better ability to share data with us. It protects them and gives them some protection when they share that data with us. That has been very successful.

We have also improved our ability working with industry to look at the supply chain, risk management. I won't get into everything we have done there, but what basically done is we are sharing it, and we are putting some systems in place with industry to be able to see that data better.

We have now included working very much with industry to include now language that is in all IT [information technology] and cyber contracts that requires certain levels of security and reporting. All of those things are beginning to show results, and one way

that we impose costs on them is to raise our basic level of cyber defense and make them play much higher to play the game. The things we are doing I believe we are now starting to see some effects in that area about who isn't playing as much anymore and what they are having to pay to play.

Mr. LANGEVIN. Thank you. So I have been examining the practices and techniques that the financial sector is using to determine and address the cyber risk of their contractors and vendors, and in many ways, they are way ahead of what the government is doing.

To what degree have you cribbed from civilian sector best practices?

Mr. HALVORSEN. Sir, very much so, and I would say that we share a lot. In the financial sector, in particular, they have just published some new standards about what they expect from their vendors. If you looked at what they wrote and you looked at what we wrote in our ours, they are very similar. That was actually a fairly collaborative effort with the financial industry.

We are also doing that with other segments of industry, with the logistics companies and other things. So we are cribbing a lot from industry. I spend a lot of time on our mobility policy. We will see, as that comes out, that will be completely again written with industry playing right from the beginning to help us get those pieces right so that we get the advantage of effectiveness and efficiency while we are using industry practices to raise the level of security.

Mr. LANGEVIN. Can you describe for us the Department's progress on the creation of persistent training environments of the type and scale necessary to conduct group and collective training, rehearse missions at the unit level, as well as integrate and exercise the full spectrum of national, state, local, and private sector capabilities?

Admiral ROGERS. So we identified that as a core enabler for us to build the vision, actually create the capability we think we need. In fact, this is one I actually—Deputy Secretary Work and I worked directly on this—and where I said: Hey, boss, I could use some more help here in fiscal year 2015. He was kind enough to generate additional funds for us. We have created a capability down in Suffolk, Virginia. In fact, we have been using it now every year with the Guard and interagency to look at how we can model different scenarios where DOD would be applying the capabilities to support critical infrastructure.

In addition, we generated the capability at the Fort Meade area that we can increasingly pour it out across the framework for us. This has been a big investment area. You see it on the 2016 budget as well. We thank you for your support for that.

Secretary WORK. In our PB17 [President's budget 2017] build, Congressman, Secretary Carter has again defense of the networks is number one. Improving training is right up there. So this is going to have a very, very high level of attention from the top down.

Mr. LANGEVIN. Thank you all.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

As I mentioned to our witnesses earlier, Mr. Smith and I have to go testify ourselves in front of the Rules Committee, so I am

pleased to yield the chair—and yield for questions he may submit—to the chairman of the Emerging Threats and Capabilities Subcommittee, Mr. Wilson.

Mr. WILSON [presiding]. And ladies and gentlemen, it is the unique situation where I have just been recognized and I get to preside simultaneously. But it really gives me an opportunity to thank Chairman Mac Thornberry and Ranking Member Smith for their planning this week, cyber week. It is really a recognition for our three witnesses how important what you are doing, protecting American families. And so I am very grateful we had a hearing yesterday on cyber threats to American families, our national defense.

We have this hearing. Later this afternoon, we have a briefing. I want the American people to know that we have got really good people, like Congressman Jim Langevin, all the way from Rhode Island, who is the ranking member of the Emerging Threats Subcommittee. This really is a bipartisan issue that we face of great concern of attacks on our government, on private businesses, on American citizens, and what you are doing is so important. We have also got extraordinary staff, people who are here working on these issues.

And, again, each one of you, in your capacity, are making such a difference, and we look forward to working with you in the future. In particular, Secretary Work, during the cyber hearing yesterday and the chairman mentioned in his opening statement about the concept and proposal of hack-back; for example, when a private company takes retaliation into their own hands and hacks back at someone who has attacked our networks or systems. Can you outline concerns that you have? And is hack-back inherently a government function that only the government should do? Or is there a private role?

Secretary WORK. Well, this is a very, very important issue for us because cyberattacks often have second and third and fourth order of consequences that we really have to understand, that they may cause escalation that were unintended. So this is an extremely important policy question for us as a nation to grapple with.

Admiral Rogers deals with this on a daily basis, and I would ask him to provide some specifics.

Admiral ROGERS. So I not only acknowledge the policy complications, but I also try to point out, at an operational level, we have so many actors in this domain already, adding more only complicates things.

The second and third order effects, as the Secretary has outlined, are of significant concern. And so I have, from my perspective, urged be very careful about going down this road because I don't think it is one that we truly understand. And from my perspective, the potential to further complicate an already complicated situation is very significant here.

Mr. WILSON. And as complicated as it is, I am just so hopeful that with the expertise that you have, to me, it would be a deterrence with some level of hack-back. And so I hope this is pursued and the capable people that you are and that you have working with you, I can't wait to hear of their capabilities as to deterrence, stopping hacking on American families.

And, Mr. Halvorsen, the Department recently issued a new manual for the defense support of civil authorities, which for the first time addresses cybersecurity related incidents. Could you discuss how DOD gets a request for such support, especially if it might be coming from a State or local agency?

Mr. HALVORSEN. Yes, sir. As the manual lays out, there are some formal processes we would go through with that, but one of the things I want to stress is the informal processes that we have put in place. We have now scheduled routine meetings with industry CISOs [chief information security officers]. My CISO, Richard Hale, who you will, I think, hear from later today in a closed hearing—had scheduled meetings with their security officers, both officially and unofficially. So we are sharing that data. We are moving forward to be able to give them some of our data quicker.

Mike's work has been superb in being able to lower the classification levels of data so that we can share that much quicker with industry and accept theirs in a similar fashion. So I think all of those things plus what is in the manual are adding to our—all of us, industry and the government's—collection of data and what I will call operational intelligence that we can use to better security.

Admiral ROGERS. And I would also add, this is an issue where we collaborate very closely between the Northern Command commander, U.S. Cyber Command, the Department of Homeland Security, the Guard and Reserve, the FBI, about how can we make sure that we are most efficient about how we are going to apply DOD capacity within the cyber arena within the broader defense support to civil authority construct because I am trying to make sure, can we use that existing framework to the maximum extent possible as opposed to trying to create something new, something totally complex in the cyber arena?

Mr. WILSON. Admiral, thank you for being—pitching in. I want you to know, as a very grateful Navy dad, with three sons in the Army Guard, but I am very grateful for your service and naval service in general.

Secretary Work, in your testimony you stated, quote: "The Iranian actors have been implicated in the 2012, 2013 attacks against U.S. financial institutions and in February 2014, last year, cyberattack on the Las Vegas Sands Casino."

What economic sanctions or legal actions resulted from this activity? Are they being maintained?

Secretary WORK. Sir, I am going to have to take that for the record. I don't know exactly what sanctions the DDOS [distributed denial of service] attack that you referred to against the financial services was attributed to Iran, as well as the Sands Casino, as you said. I am going to have to get back to you and say exactly what we did as a result of those two attacks, but Mike might know.

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

Admiral ROGERS. No specific sanctions tied to those each individual discrete events. It is clearly a broader discussion about what is acceptable, what is not acceptable. We have seen a change in behavior. The activity that we had seen previously directed against financial Websites, for example, has decreased, in part, I think, because of the broader, very public discussion we were having in

which we were acknowledging the activity, and we were partnering between the government and the financial sector to see what we could do to work the resiliency piece here to preclude the Iranian's ability to actually penetrate, which, knock on wood, we were successful with.

Mr. WILSON. And, again, thank each of you.

We now proceed to Mr. Larsen of Washington State.

Mr. LARSEN. Thank you, Mr. Chairman.

Any of you can answer this question. I am curious, though. Are we still exploring what the outer limits of what constitutes the equivalent of a physical kinetic attack against the U.S. when we are looking at cyberattacks? We still know what would be the equivalent kind of cyberattack that would warrant the kind of and size of response that we might do if there was a physical kinetic attack against the U.S.? We exploring the outer limits still?

Secretary WORK. Well, we defined an event of significant consequence, it has to include either a loss of life; significant damage to property; serious adverse U.S. foreign policy implications or consequences; or serious economic impact. Now, that is a broad statement, and each of them have to be addressed as an individual act, and that is why there is no established red line on what we would say this constitutes a physical attack.

The question we are often asked is, when does a cyberattack trigger an act of war? And each of those would be discussed in turn, depending on the type of attack and what its consequences were. As of this point, we have not assessed that any particular attack on us has constituted an act of war.

Mr. LARSEN. Can you—and Admiral, you addressed this a little bit—be more specific about the title 10 versus title 32 responsibilities in working with the National Guard or even going beyond that, working with either national, State, or local law enforcement? What specific criteria do you use to make that distinction?

Admiral ROGERS. For me, among the things I look at our scope of the activity we are dealing with, the nature of the event that we are trying to deal with, capacity that exists within the title 10 arena versus in the title 32. Are there specific knowledge or unique insights that, for example, a particular Guard structure might have that are really well tailored to deal with this specific issue?

Again, it is a case-by-case basis. The touchstone, though, I have tried to maintain with my Guard teammates and the States is we need one integrated workforce between the Active and the Reserve Component, trained to the same standard using the same basic scheme of maneuver so that we can use these capabilities interchangeably. That maximizes our flexibility as a Department, and it gives us a broad range of options in terms of how we employ the capability.

Mr. LARSEN. And then are you making that largely permanent? At some point in the future, you have moved on to something else, and someone comes in behind you? So is this still evolving, how you are trying to establish these relationships as they apply to cyber, or are these going to be largely permanent? Will you be changing the story?

Admiral ROGERS. Right. I think they will be largely permanent. I feel pretty good that we have done the foundational work, if you

will, broadly. I always remind people: Remember, no plan ever survives contact. And the broad framework we are going to acknowledge as we get into this, we are likely to see things we hadn't anticipated, and we have got to be flexible and be willing to change as we need to given the specifics of whatever particular event it is that we are dealing with.

But I would compliment the Guard and the Reserve for the way we have partnered on developing the cyber capability within the Department. It hasn't been adversarial at all. It has been a great team.

Secretary WORK. In fact, I would like to jump in on that, sir. We work very closely with the Council of Governors. I would like to give them a shout out. We have been dealing with this on how to build up cyber capacity in the Guard and Reserve. We are building right now toward about 2,000 Guard and Reserves that are associated with this. And what we are doing right now is trying to work out the policy on what our folks can do in terms of coordination, training, advising, and assist under title 32 and title 10 authorities.

That is actually—the policy—is working well. We are working well with the Governors, and we believe that this is going to be a great new story for the Nation.

Mr. LARSEN. Right, that is nice. In my last few moments here, I have a question. We talked about defensive networks—defense of networks, that is—talked about resilience, denial, and the whole deterrence issue, but this issue of hybrid warfare, of course, has come up and I am curious about what steps you are taking to incorporate in a U.S. response or even in NATO's [North Atlantic Treaty Organization's] response and the role CYBERCOM plays in this in incorporating a responsive capability within this hybrid warfare concept that we hear really a lot out of General Breedlove.

Admiral ROGERS. So, it is a concept—we are partnering both with General Breedlove at EUCOM [European Command] as well as in his NATO role as the Supreme Allied Commander, and it also highlights the work that Special Operations Command, that General Votel's team are doing in this regard. In fact, I was just down in Tampa about 10 days ago. This was part of our broad discussion about how do we integrate the full range of capabilities within the Department as we are trying to respond to an evolving world around us?

I think we are starting to have some good conversations in a good broad way ahead within the Department. The international framework for this is little more difficult. I think it is fair to say not as far as advanced, for example, with us and NATO. It is an area we have talked about we have got to work on.

Mr. LARSEN. My time is up. Thank you very much.

Mr. WILSON. Thank you, Mr. Larsen.

We now proceed to Congressman Doug Lamborn of Colorado.

Mr. LAMBORN. Thank you, Mr. Chairman.

I appreciated your comments to earlier questions that were directed from Congresswoman Susan Davis, but I would like to follow up and build on that. This concerns recruiting and retaining top talent. So what are your efforts to—and this is for you, Admiral

Rogers, in particular—what are your efforts to develop a unique cyber career track for those in the military?

Admiral ROGERS. So, services have the responsibility for man, train, and equip within our Department, in terms of they generate the capacity I employ then as the joint commander. In the cyber arena, though, one of the things that has been a real strength is the joint world and the services have been totally integrated as to how we are going to develop this, what are the standards, what are the skills, how do we create that workforce. And that is what I did, in fact, in my last job. I am very comfortable with how each service has tried to create a career path that enables us to extend over an entire career both this capability as well as generate the insights we need in the workforce. I think that is a big change for us over the last 5, 10 years. I think it is a real strength for the future. It is not an area that I look at now and I go: Wow, I have real heavy concerns there. I think we have got a good way ahead and a good broad vision, and the capacity and the capability of that workforce, I have yet to run in—knock on wood, with my luck, this will happen tomorrow—but I have not yet run into a scenario where we didn't have the level of knowledge.

The challenge has been I might have had a handful of people with the right level of knowledge, but we had people with the knowledge. I have got to build that capacity out more so we have got more of it, if you will.

Mr. LAMBORN. Okay, well, I appreciate hearing that and that is really encouraging, so thank you.

And Secretary Work, the Department has recently floated a number of new civilian and military personnel reforms, compensation, retirement, et cetera. How will some of these reforms affect the cyber workforce?

Secretary WORK. Well, I actually was going to try to jump in here because this is a huge priority for Secretary Carter. He came into the Department believing that over time we have created these barriers for service in our government. And he wants to really, as he talks, burrow tunnels through these barriers or widen the aperture. And he uses cyber as an example of new ways in which we might bring people into the government and allow them to serve for a while, then go back out into the civilian workforce, and come back in. And so he has challenged us and the Under Secretary of Defense for Personnel Readiness, Brad Carson, on this force of the future to say: How can we make sure that in areas like cyber, you know, space, electronic warfare, we have more permeability in the Department to make sure that we are getting the best ideas from outside the Department?

I don't have any specifics to give you right now because they are in the process of going through a deliberative, "Which ideas are good?" But we are right with the intent of your question to improve the ways in which people can come in and out of our government service because, as Mr. Halvorsen said, this is an exciting mission for many, many people. And maybe they don't want to make a 30-year government career, but if they had a chance to help Admiral Rogers for a 2- or 3-year period, they are all in. So we have to improve the way to do that.

Mr. LAMBORN. Okay, thank you.

And, Mr. Halvorsen, do you have anything to add to what has already been said?

Mr. HALVORSEN. No. I just echo all of the same comments.

And while we are waiting for some of that to be staffed, you heard we are moving forward on some pilot programs to bring industry into the government, for us to put, for the first time, civilians out in industry. Those pilots are moving very well, and as we have used those to inform Brad in his work, I think you will see some great things coming out of this.

Mr. LAMBORN. Well, I thank you for your answers. And most of all, thank you for the great work that you are doing.

Mr. Chairman, I yield back.

Mr. WILSON. Thank you, Mr. Lamborn.

We now proceed to Congresswoman Niki Tsongas of Massachusetts.

Ms. TSONGAS. Thank you all for being here. It is obviously a topic of great importance. And I think, as you said, so much of this is about personnel, really being able to attract the people and keep the people who have the skill set and the commitment to thinking this through because it is not easy stuff—that is for sure—at all. And I gather from the testimony I have heard that there is a fair amount of comfort level with what DOD and the military services have been able to do to put in place appropriate means of training, hiring, and then compensating, even though you have said you may have to come back to us in the future.

But you also commented that this is sort of an interagency effort and you are working with the Department of Homeland Security, law enforcement, the FBI, the Intelligence Community. How much sharing across those borders is taking place in terms of the skill set that you need in each of those aspects of this effort and how comfortable are you with the ways in which you are working together and how they are responding to the challenges they face in terms of personnel?

Admiral ROGERS. I mean, I would argue very well.

For example, this is one I have personally sat down with the director of the FBI and talked about: Hey, are there things we could be doing together? It is a conversation I have had with the leadership at Homeland Security. It is a conversation, quite frankly, I have also had with the private sector, where I have argued: We are both competing for the same pool. What works for you? What might we be able to do differently? Are there ways, as you have heard previously, can we partner?

I would make just one slight twist because this is a point I wanted to make today. I would tell you, on the opposite side, though, the single greatest perturbation I have experienced within my workforce in 18 months has been even the hint of a shutdown. In the last week, I have had more agitation out of the workforce arguing this would be the second time in 2 years. And we are even having this discussion—hey, even if we don't shut down the government, just the fact that we are even getting this close, the workforce is very open with us about, "I am not so sure I want to be part of an organization where there is this lack of control, and I can't count on stability." That really concerns me because I can't overcome that.

Ms. TSONGAS. Secretary Work, do you have any——

Secretary WORK. Well, this is a very competitive field, as the admiral said. We are building up a total of 133 cyber teams in the Cyber Mission Force. Some are focused on protection of the networks. They are called Cyber Protection Teams. Some are focused on national infrastructure protection. They are called the National Mission Teams. Then we have teams that are supporting our combatant commanders. We want to build to a total of 133 of these teams. It is going to be about 6,200 Active Duty military, civilians, and in some special instances, contractors, and we won't get there until 2018. So we are in the process of building these.

And this is a very competitive space. We are on track. We are doing well in our recruitment. But as Admiral Rogers says, any hints of shutdown or sequestration, that will really set us back. So we think we have got a good mission that people want to participate in, but we are not where we need to be yet, Congresswoman, and we still have until 2018 to build up the force to where we just think is the minimum necessary to do our missions.

Ms. TSONGAS. You know, I serve on the board of one of the service academies, the board of visitors of one of the service academies. And I know in our discussions, we have heard that it has been difficult to attract young airmen, in this instance, to the cyber field because they come into the academy with a particular idea in mind of where they want to spend their time. And so it is not always as simple as we would like to think, given the extraordinary challenge.

But I have another question as well. You know, the Department has shown its commitment to leveraging private sector cyber innovation, and we have heard about that here today. I commend Secretary Carter with making his way out to Silicon Valley to create some presence there, a satellite campus there, to have a way in which to interact more easily with that community. And I just wonder, how will you expand that program and look to other parts of the country where you have a deep bench of cyber activists, cyber innovators, cyber experts?

Secretary WORK. Well, if you are referring, Congresswoman, to the Defense Innovation Unit-Experimental [DIUx]—and it is an experimental unit. We want to see how we can interact with the private sector in the best way. So, for example, one of our ideas was to bring people back to the Pentagon and show them what we are doing. And they said: No, really what we want to do is go to the field and see what your airmen, soldiers, marines, and sailors, what do they do? We want to go on ships. We want to see what their problems are. We want to help them.

So once we do the lessons learned there, we expect that to be successful, and it will become a permanent unit. And then where would we expand? We would go to other innovation centers throughout the country, perhaps Boston. There are different places. And Mr. Halvorsen has been helping us to think through this also.

Mr. HALVORSEN. You know, as the Secretary went out to Silicon Valley, we had also taken a CIO team to Silicon Valley. In December, we are doing a similar thing in Boston and New York. And not just waiting for that, we have hosted just recently a group down from Boston and New York, both some of the more mature cyber

companies but also a group of some of the innovative companies. I think what we are trying to do with DIUx is really take what Silicon Valley stands for, not the geographic location, and make sure—and the Secretary is very clear in his guidance—so is DEPSECDEF [Deputy Secretary of Defense]—to us to: Hey, it is more about the concept of innovation. Reach to wherever that is, and it is not just in Silicon Valley. So you will see us in the next couple of months spend more attention in the Northeast and, frankly, in the Southwest sector.

Ms. TSONGAS. There is really no substitute for physical presence and the kind of physical interaction, day-to-day interaction that can take place. Thank you.

My time is up.

Mr. WILSON. Thank you, Ms. Tsongas.

We now proceed to Congressman Mo Brooks of Alabama.

Mr. BROOKS. Thank you, Mr. Chairman.

At Redstone Arsenal, next to Huntsville, Alabama, the Army is establishing a cyber campus within the Aviation and Missile Research, Development, and Engineering Center, also known as AMRDEC. This campus consists of qualified cyber personnel and facilities to provide world-class cybersecurity support to aviation missile systems by using cutting-edge research and development of cybersecurity solutions to challenges associated with emerging and legacy technologies.

The AMRDEC cyber campus coordinates cyber activities with industry, academia, and government partners. Although an Army asset, it is uniquely positioned to integrate the Department of Homeland Security, the Department of Justice, the Space and Missile Defense Command, and the defense industrial base. Additionally, it can provide deep technical expertise and reduce the risk of cyber threats posed as it relates to hardware, software, firmware, networks test and evaluation, modeling simulations, forensics, industrial control systems, supervisory control, and data acquisition systems. With that as a backdrop—and these questions are for each of you—How does the Army's vision with AMRDEC integrate with the Department of Defense's overall cyber strategy?

Secretary WORK. Well, as Admiral Rogers said, each of the services are developing cyber skills within each of the—under their title 10 responsibilities. And this is just one reflection of many, many, many such organizations that are being set up. The Air Force has units down in San Antonio.

And so I would ask Admiral Rogers to give you more specifics, but each of these are going to have specific skills. In this case, the one that you have talked about, Congressman, really focuses on the aviation systems of the Army and how they can make sure that they are not vulnerable to cyberattack, but they develop other skills, too.

Admiral ROGERS. So every service, as the Secretary indicated, is developing a similar kind of capability, similar kinds of relationships. Army has chosen to really harness the capability resident at Redstone in the northern Alabama area. The positive side thing for me is we have got a good, strong collaboration across the services as to who is doing what and where. The question I think increasingly for us over time is, as we get more experience, do we need

to increase investments in certain areas where we are really seeing strong results versus other areas where perhaps it hasn't played out as well as we would like? And we are going to generate more insights in that over time.

Mr. BROOKS. Thank you.

Mr. Halvorsen, would you like to add anything?

Mr. HALVORSEN [continuing]. The policy absolutely talks about how we do better with industry, and part of what that unit is doing is bringing in industry in the area, too, to be part of the solution to the problem. So I think they are perfectly aligned with what they said and what was in the policy.

Mr. BROOKS. Okay, a followup question. Is there a consolidated effort to ensure cyber centers, such as the one at Redstone, are interconnected with other services and Department of Defense capabilities to properly leverage knowledge sets and not create stovepipes of information or efforts?

Admiral ROGERS. I don't know that we have a formal—I know there is regular analytic and collaborative venues where they all get together. I participate and my team participates in some of those. I don't know that there is a formal process, if you will. I try to synchronize that at my level with each of the service components that work for me about: Hey, we have got to look at ourselves as one integrated enterprise here, guys, because we have got to maximize effectiveness and efficiency because there are more requirements than there is money and time, so it is all about, how do we maximize outputs?

Mr. BROOKS. Mr. Work.

Secretary WORK. Sir, I don't believe there is a formal program right now. We look at it more in terms of function. So, right now, I can tell you in terms of defense of networks, everything is on the same playing field. We all have the same score cards. We all grade ourselves exactly the same. But to your specific question on whether or not we have a formal program, that is something I will need to go back and research and say—it sounds like a good idea. I just don't know exactly how we would implement it yet.

[The information referred to can be found in the Appendix on page 74.]

Mr. BROOKS. Mr. Halvorsen.

Mr. HALVORSEN. Like Secretary Work said, we will have to go check and see. It sounds intriguing.

Mr. BROOKS. Thank you, gentlemen, for your insight.

Mr. Chairman, I yield back.

Mr. WILSON. Thank you, Mr. Brooks.

We now proceed to Congressman O'Rourke of Texas.

Mr. O'ROURKE. Thank you, Mr. Chairman.

Secretary Work, you were talking about the three basic tenets of deterrence. And the first two, denial and resilience, I understand pretty well. There have been a number of questions about the third one, which is cost imposition. And I am interested in knowing how we communicate or advertise the consequences of cyberattacks to potential adversaries, and to the degree that you can talk about it, how has that changed their behavior? And how have some of the consequences that we have imposed thus far changed their behav-

ior? In other words, how have we done on that third tenet, on cost imposition?

Secretary WORK. The first is to have a strong policy statement that we will respond at a time, place, and manner of our choosing. And then we have to communicate, primarily with state actors. I think Admiral Rogers said yesterday, we are pretty good at stopping 99.5 percent of the attacks, you know, getting rid of the basic hacker, but it is the state adversaries that pose the biggest challenge.

And I would just like to weave in—I think the chairman mentioned the Xi and—President Obama and President Xi, the cyber agreement. And that came about from intensive discussions with the Government of China saying: This behavior is unacceptable, and we have got to come to grips with it. So there were four specific aspects of what I would consider this, call it a confidence-building measure.

The first one is that we have to have timely response for information and assistance if we go to China and say: Hey, there is an actor inside China that is conducting these activities. We have agreed to share that information. Both the United States and China have agreed that they will not knowingly conduct cyber-related theft of intellectual property for commercial gain. We are making common effort to develop these norms of state, norms of behavior, which we have never done before. And then we agreed to a high-level joint dialogue.

Now, people say: Whoa, there is no enforcement mechanism.

But it is a confidence-building measure, and it is the first time that the President of China has said: I will commit my government to these things.

We believe it is very, very significant and could lead to this. And it came about from high-level dialogue where we were saying: We find your behavior unacceptable. And we do have options. But how can we work this out?

So I believe in the Sony case, we attributed. We did sanctions. I believe that those types of activities will prove that the United States is very serious about this and may lead to these better norms of behavior between nation-states.

Mr. O'ROURKE. I think that is the hope. What are you actually seeing in terms of changed behaviors? I understand the agreement, which is important, and the statements of intent. What are you seeing in terms of number and severity of intrusions or cyber-attacks following, you know, letting our adversaries know that we will choose the place and time of our response? And having responded in some of these cases, what has that done?

Admiral ROGERS. So we are in an unclassified forum, but in broad terms——

Mr. O'ROURKE. To the degree you can.

Admiral ROGERS [continuing]. You haven't seen the North Koreans attempt to engage in another offensive act against the U.S. infrastructure since November of 2014, and the aftermath of our economic sanctions and very public attribution and discussion. I would argue, in at least the denial-of-service activity we saw the Iranians, for example, doing back in the 2012, 2013 timeframe, we have not observed that of late. I would argue for other nation-states, the im-

pact to date has been—I am not seeing significant changes. Again, it is early with respect to the PRC [People's Republic of China]. We need to see how this commitment plays out over time, and trust me, we will be paying great attention to how this commitment plays out over time.

Mr. O'ROURKE. I think that is something that I and perhaps other members of the committee would be interested in receiving a briefing on going forward, just to look at how behaviors are changing and whether that third tenet of ensuring that our adversaries understand the consequences and costs of these kinds of attacks, making sure that that is really working. So I appreciate your answers.

Mr. Chairman, I yield back.

Mr. WILSON. And thank you, Mr. O'Rourke.

We now proceed to Congresswoman Jackie Walorski of Indiana.

Mrs. WALORSKI. Thank you, Mr. Chairman.

Admiral Rogers, I have a question. You said earlier that Russia is a peer competitor in terms of our cyber technology and the cyber threats that are out there, and I guess I am interested to see what your perspective is. I am just sitting here and I have been watching through the course of this hearing the Russian bombers that let loose today in Syria with 1-hour notice to our generals in Baghdad and striking non-ISIS [Islamic State of Iraq and Syria] targets. And I think this is a reprehensible activity that is happening today, and I have many questions as to how we ended up here.

But I am curious from you, with this development today of an overaggressive Russia, how in the world do we go forward with talking about peer competitors and sharing intel information and trusting anything that comes from Putin in Russia?

Admiral ROGERS. Well, clearly, your point is much broader than the cyber arena that I am talking about.

Mrs. WALORSKI. I think it is completely related.

Admiral ROGERS. Okay, I didn't say it was unrelated. I said it was broader. One of the points I try to make is you have to remember that cyber happens in a broader strategic context, so it is important that we understand the broader strategic context.

Mrs. WALORSKI. Would there not be an element of trust that would have to prevail here when we just literally saw what happened this morning, and for many of us that have sat here on this committee for a long time, saw a red line that was violated and not upheld in Syria. We have seen all of these different gaps with all of these different countries around the world with an administration that seems to not have any kind of a strategy or a contiguous plan. How would we take a step forward today? I know you are looking at the broad context—or you are talking about the broad context, but I don't understand the gap that is going to be there—that has already been there, but the gap that is going to continue to emerge today, how in the world do we breach that and how in the world do we say to the American people with all seriousness and looking our constituents in the eyes that we have their back and that we are looking out for the security of the United States of America and our allies and we are watching Vladimir Putin come right into the Middle East right next to our cohort and friend that we want to protect, Israel—does that not change the equation

of trusting or having any kind of semblance of trust with Putin and Russia?

Admiral ROGERS. Well, I would only argue this latest issue fits in a broader context with the Ukraine and others. This is not a new phenomenon in many ways with this particular actor. It is why we have been very direct with them. I know the Secretary has had conversations with his counterparts in the Russian framework. I have not had specific cyber discussions with them. I will say, one of the points I try to make in our internal discussions is: I am watching the Russians use cyber in an ever-increasingly aggressive way.

Mrs. WALORSKI. And would this not be a major alarm? This is alarming to me that he just talked to the President yesterday and evidently said, "Stay out of our airspace," and we get 1 hour of warning. And they go in and they attack Syria. So now they are a main state player as we are screwing around in our country. We are fighting back and forth over all kinds of things right now. We just had the Pope here. And while America's distraction is focused over here, it, seemingly, is that he is using a phenomenal window of opportunity to go in and be another major push in Syria. And the alarm, I think—not only for lawmakers today but for the citizens of our country that we are vowing to protect—is we have now watched him establish himself in Syria, in the Middle East.

Secretary WORK. Obviously, as outlined by President Putin, he believes he is following his national interests. We are alarmed by what happened this morning. What was agreed by the two Presidents is that our militaries would talk so that we would deconflict operations.

Mrs. WALORSKI. So have we not seen a failure between our President and President Putin if we were going to talk and try to avoid something like this? Because now he is there 1 hour, 1 hour of notice, with all of our forces over there, the allied forces, the NATO forces, the other nations that are fighting as well? I mean, would we not see this as a failure?

Secretary WORK. I don't believe it is a failure. I believe it is an aggressive action by Russia right now in advance of our discussions between our two militaries.

Mrs. WALORSKI. And are you confident that we have a strategy with the President of the United States that just met with Putin? Are you confident that those two leaders have a strategy and that we are holding up our end of the bargain? Are you confident that the administration is looking at this as, "Oh, well, we expected this to happen"? I look at it as a gigantic breach because I represent three-quarters of a million people that are looking at their TVs right now like I am, and the official response from the Pentagon, "taken aback by strikes." I think we are all taken aback. Is there a strategy that was supposed to prevent this, or is our attitude now, "Well, we know they are going to do their things; we are just going to see at what point we are going to try to contain them"?

Secretary WORK. We have a disagreement on strategy. They want to be able to do military action first followed by a political agreement.

Mrs. WALORSKI. They are doing military action. They have been doing military action. They encroach on the Ukraine, they are mak-

ing headway through that whole Eastern European area. They have been doing military action, and today we are watching a live bombing, and from your perspective and the perspective of the administration, we expected that? The American people don't. I don't expect that.

Secretary WORK. The Russians made clear that they would support the Assad regime with air strikes, and we made an agreement to have our militaries talk so that there would not be any problem between our interactions between our forces.

Mrs. WALORSKI. You think 1 hour of notice is legitimate for two organizations and militaries that are talking? Obviously, talks broke down, and we got a last minute—so what is our response now?

Secretary WORK. Well, you have me at a disadvantage, Congresswoman. I don't know exactly what has happened over the last hour. We heard about the attacks this morning. They asked us to avoid the area where they would be operating. We continue to fly throughout Syria.

Mrs. WALORSKI. And we continue to talk. Are we continuing to talk to our Russian counter-opponents?

Secretary WORK. We have agreed for our militaries to meet, and that meeting just simply has not occurred. It was an agreement between the two Presidents just a couple of days ago. So we are trying to find out where we will meet, where it will be, who——

Mrs. WALORSKI. Would you not agree this is a crisis because for the first time, they have now entered the Middle East. And for the first time, we now have watched the broadening of Putin's powers, who was just here on the American soil right next to a mess, a hotbed of war, and right next to our dear ally Israel. Have we not now watched something elevate to the point that this is now a crisis because Russia has just now gone from their position, through the Ukraine, looking at Eastern Europe, and now has sufficiently landed themselves with a coalition inside of Syria?

Secretary WORK. I do not believe it is a crisis. I believe it is a disagreement in strategy, and that is what we are trying to work out.

Mrs. WALORSKI. And I respect that. I believe it is a crisis. I believe we have had a President with no foreign policy whatsoever. We have had red lines talked about and crossed. And this thing has played out all by itself, and now today here we are, back in a crisis, back on TV in front of every single American, wondering who in the world is defending our country?

And, with that, Mr. Chairman, I yield back.

Mr. WILSON. And thank you very much, Congresswoman Jackie Walorski.

We now proceed to Mr. Takai.

Mr. TAKAI. Thank you, Mr. Chairman.

I would like to rebalance and refocus to cyber strategy, if I may. A lot of my colleagues have asked about deterrence today, and this is something that I am also very concerned about after recent events that have been discussed. With the current threats to our cyber network, the need to discuss here today, including creating and maintaining a persistent training environment, development of a unified platform, and building the Joint Information Environ-

ment to secure the DOD enterprise, the development of these priorities cannot only serve as a deterrent in their own right but will enable our CYBERCOM—our Cyber Mission Force readiness to be the best in the world. So, Admiral Rogers, where is DOD in allocating resources for these priorities? If you could address each one, again, persistent training environment, unified platform, and the Joint Information Environment.

Admiral ROGERS. So persistent training environment is a program that we have put together. It will take us several years to finish. I think we are in the—fiscal year 2017 represents the third year of funding for it. We are working through the 2017 build now internally within the Department. Again, I sense strong support for this. I haven't come to an issue yet where I am saying, "Oh, I have problems with the way ahead."

I think we have got a way ahead, and it seems to be working. JIE [Joint Information Environment], I will let Terry comment only because it has been a particular focus for him.

Unified platform, a relatively new idea for us that, based on 5 years of practical experience now as an organization, we think the Department needs to create a capability somewhat separate from NSA [National Security Agency], if you will, for us to execute operations. Unified platform is the program name we put together in terms of our ability to do that. Again, we really are starting that with the 2017 build. And it is an example to me of how, as we gain more experience, as we do this over time, we have got to continually reassess and ask ourselves: So are some of the assumptions that we made when we started, are they proving to be what we thought they were, or do we need to make changes?

Mr. TAKAI. Okay, and the——

Admiral ROGERS. JIE, if you want to——

Mr. HALVORSEN. With respect to JIE, the first concrete action that becomes of that is the establishment of the Joint Regional Security Stacks [JRSS]. They are on track. They will be funded in 2017, and they will be fully operational by the end of 2017.

Mr. TAKAI. Okay. Thank you. I wanted to go back to the integration of personnel. I know the Secretary mentioned that, and I think you, Admiral, as well, I want to focus on defining where the role of the National Guard fits into the cyber strategy. I am a member of the Guard in Hawaii, and all of us here on this committee have constituents in the Guard. So can you touch upon some of the points on where the Guard can increase their role in the larger cyber mission?

Secretary WORK. Let me just start by saying, our cyber force that we are building to as we discussed earlier, Congressman, is about 6,200 Active and civilians and, in some special cases, contractors.

Mr. TAKAI. Right. That is what you said. You didn't mention National Guard when you said that.

Secretary WORK. Two thousand—2,000—National Guard and Reserves on top of that. Some of them will be part of the cyber teams that I talked about, and others will be extra capacity that might be able to help the States. As I said, the Council of Governors and we have been working very, very closely together. Our policy shop is working through all of the aspects of what we can do under title 32 and title 10 authorities in support of the States. But the Guard

and Reserve will be absolutely central to the Cyber Mission Force; about a quarter of the entire force, 6,200 in the Active side and another 2,000 on the Reserve and National Guard. So they are absolutely central.

Admiral ROGERS. The only other comment I would make, and I say this, I am the son of a guardsman. My father was a member of the Illinois National Guard for 27 years. So, as a child, I watched him every day, every month, every summer participate in Guard activities. And I spent a lot of time playing in armories as a little boy every day with my father.

Every service has used a slightly different construct. In the case of the Air Force, they are using the Guard and the Reserve to fill out a part, if you will, of the Active requirement for their share of the 6,200. In the case of the Army, they have decided that the Guard and the Reserve represent an opportunity to generate additional capacity over and above that dedicated 6,200 people. Clearly, Navy and Marine Corps don't have a Guard construct. It is a little different for them. But as I have said, the discussions today have been very good. I think, as the Secretary said, we have got a way ahead in terms of how we are going to work our way though this, particularly this, quote, "additional capacity," if you will, that the Guard is developing and partnering with the States about how we are going to view this as one integrated enterprise, as it were, so we are maximizing the capabilities that the Department and the States are investing in.

Mr. TAKAI. You spoke earlier about the cyber teams and the number of teams that you are building. I understand that there may be, in fact, opportunities for these teams to be wholly Guard. You didn't mention that today. So can you——

Admiral ROGERS. I said in the case of the Air Force, for example, a portion of their share of the 133, they, in fact, are creating a small number of teams that are wholly Guard.

Mr. TAKAI. Okay. Great. And then one more question for the Secretary. How resilient are our military networks to cyberattacks, and how do you measure and qualify resilience?

Secretary WORK. We are getting better, but we are not where we need to be. That is why Secretary Carter has said defense of our networks is absolutely job number one. Now, that will come through a whole lot of different things, as I said in my opening statement. First, get the network as defendable as possible. So the JIE that Terry Halvorsen talked about and the Joint Regional Security Stacks will take 1,000 defendable firewalls down to less than 200. A whole bunch of different—I mean, the number of enclaves—and Terry can talk about this—will be dropped.

So the first thing is to make your network with the surfaces, the fewer surfaces as possible and as defendable as possible. The second is to build up these teams so that is another big part. And the other one is to have a cyber scorecard, which is telling us exactly how well we are doing. And Mr. Halvorsen was the creator of the scorecard, and I would ask him to be able to tell you how we are going to track this.

Mr. HALVORSEN. So cyber resiliency is actually a measure on the scorecard that we are actively developing. It will look——

Mr. ROGERS OF ALABAMA [presiding]. The gentleman's time has expired.

The Chair now recognizes himself for questions.

Secretary Work and Admiral Mike Rogers, good to meet you. Do you use telecommunications—and either one of you—telecommunications equipment manufactured by Huawei in your offices?

Admiral ROGERS. I apologize. I didn't hear the question.

Mr. ROGERS OF ALABAMA. Do you use telecommunications equipment manufactured by Huawei in your offices?

Secretary WORK. In the office of the Secretary of Defense, absolutely not. And I know of no other—I don't believe we operate in the Pentagon, any systems in the Pentagon.

Mr. ROGERS OF ALABAMA. Admiral Rogers?

Admiral ROGERS. No.

Mr. ROGERS OF ALABAMA. Why? Why do you not use it?

Admiral ROGERS. For us, I think it is a broader conscious decision as we look at supply chain and we look at potential vulnerabilities within the system, that it is a risk we felt was unacceptable.

Mr. ROGERS OF ALABAMA. Secretary Work? Agree with Admiral Rogers. What about your cleared defense contractors? Should they be using Huawei telecommunications equipment?

Secretary WORK. I will have to take that for the record, sir. I know of no defense contractors that are using Huawei equipment, but I just don't know.

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

Mr. ROGERS OF ALABAMA. Okay.

Admiral.

Admiral ROGERS. This is a broader departmental issue. I mean, we don't, the contracts we have, we specify security standards that you have to meet. We specify the requirement to notify us. Again, I think we would have to take it as a question. I don't know if the current language—and Terry may know—but I don't know if the current language specifies specific vendors, if you will. You may or may not. I know in some of the national security systems, we are very specific about making that standard. In the nuclear and other areas, we are very explicit that that is not allowable.

Mr. ROGERS OF ALABAMA. Well, Secretary Work, I would appreciate if you would get back with me on whether you have any cleared defense contractors that are compelled to use Huawei telecommunications equipment.

And, with that, my next question has to do with the nuclear enterprise review that recognized that Vietnam era Huey 1N helicopters that helped provide security for our ICBM [intercontinental ballistic missile] fields are woefully antiquated and inadequate. The NER [Nuclear Enterprise Review] said that we need to get new, modern helicopters into ICBM fields because after all, we are talking about nuclear weapons.

Based on a meeting I had with the Air Force and the OSD [Office of the Secretary of Defense] a few weeks ago, I am very concerned that the Air Force acquisition approach is going to take 4 or more years to get these helicopters. Now, these are ICBM fields, and I had a hearing on this security issue and this came up, and it is

alarming, the concern that we are being told by the commanders about their security of these fields. What can you tell me about why we are looking at such a long period of time?

Secretary WORK. Well, first of all, this is an extremely high priority, and we are dealing with it right now in PBR–17 [President's budget request 2017]. Last year, the Air Force plan to replace those helicopters was to take their UH–60As, their old—excuse me, take UH–60As and upgrade them to UH–60Ls and it turned out that all of the As that were available in the force were just too old and tired. And it became cost prohibitive. And that is why the timing slid because now we will have to go and buy new-build UH–60Ms or whatever helicopter we decide, whether we decide whether we can do sole source or whether it has to be a competition.

STRAT commander, the commander of U.S. Strategic Command, Admiral Cecil Haney, has come in and said we cannot afford to wait for 4 years, and we are looking at a wide variety of measures to mitigate the problem until we can get these new helicopters built. It is a very high priority issue for us in this budget build, and I will be able to give you a little bit more information once we work through all of the different options before us.

Mr. ROGERS OF ALABAMA. Okay, well, I just want you to understand that I really believe that we should see an immediate reprogramming request for the fiscal year 2017 budget.

And, with that, I will close by saying that now that the NDAA is about to be sent to the President, I would like to talk with you offline about our new engine to replace the RD–180 as soon as we can get a chance to privately.

With that, I will yield back my time, and go to Ms. Speier for 5 minutes.

Ms. SPEIER. Speier.

Mr. ROGERS OF ALABAMA. Speier.

Ms. SPEIER. Thank you, Mr. Chairman.

Thank you, gentlemen, for your service to our country. You know, we are dealing with some very, very savvy actors in these various foreign countries that have been hacking into us. On the agreement with China, Mr. Work, you seemed somewhat elated by the agreement, and yet I have reason to be very skeptical about them complying with what they agreed to comply with. But, more importantly, I would like to ask you, what isn't in the agreement that you would have wished was in the agreement?

Secretary WORK. Well, I wouldn't characterize my reaction as elation, Congresswoman, so much as I believe it is a very good first step. It is the first time that the President of China has committed himself and his country to address the issues that have been of such high concern to our government. So I consider that a very good first step.

Ms. SPEIER. I understand that, but what wasn't in the agreement? I have very limited time. So, please, if you would, answer the question.

Secretary WORK. There were no enforcement mechanisms per se, and that, I think, is the key thing that people have pointed out. But, again, I believe this was a confidence-building measure. Now China is either going to prove that they are serious about this or

not, and then we can take actions as necessary if they prove not to follow through on their commitment.

Ms. SPEIER. Now, the OPM hack was devastating, and it is clear that China did it. They denied it. It is also very clear that they now have very personal information about many persons with top secret status. And the phishing that just went on recently of the Joint Chiefs of Staff's unclassified email worries me a great deal. Whether it is Russia or China, access to that personal information is such that if they know who your family members are or who your next-door neighbor is and they then can pretend like they are your family member or next-door neighbor, you are more apt to click on to that email, and then they can get in.

What steps are being taken to deal with phishing in terms of either requiring greater accountability by those who hold those positions who end up clicking by either punishing them or coming up with some system, so that we can anticipate that kind of phishing going on and prevent it?

Secretary WORK. I would just like to make an overall point and then turn it over to Mike and Terry. Although our adversaries have very sophisticated capabilities in this regard, almost every one of these intrusions that have occurred, have occurred because of simple operator error, bad cyber hygiene. They click on a spear-phishing attempt. So we are going after that. I would just like to say that that is the biggest problem we have right now is getting our cyber hygiene better.

Ms. SPEIER. Okay, but my point is, is there any kind of penalty being imposed on those who in a careless manner click on to them?

Mr. HALVORSEN. The simple answer is yes.

And I won't go into the specifics of what has been imposed, but yes. We have upped the level of accountability on that and actions have been taken for people who have misbehaved in a cyber way.

Secondly, we have increased the training frequency, phishing training, and we have taken certain actions on the networks to eliminate the ability to click on links. And at a minimum, we have a warning on there now that says you must think about this link, and in some cases—and again, I won't say—you physically can no longer click on links via any of our networks.

Admiral ROGERS. And I would say from a network perspective, I have implemented nine specific technical changes where, quite frankly, I have told users now, I am going to make your life harder. If this is what it takes to drive a change in behavior, I will make your user life harder to try to preclude this from happening.

Ms. SPEIER. My last question and very briefly, what is keeping you up at night?

Admiral ROGERS. So I would say from my perspective, there are three things in cyber that concern me: Are we going to see offensive activity taken against U.S. critical infrastructure? Are we going to see the focus shift from theft of intellectual property, the theft of information, to manipulation of the data that is in our system, so we no longer can trust what we see? And then the third thing that worries me is, are we going to see nonstate actors, meaning terrorist groups are probably at the forefront on my mind, start to use the Web as an offensive weapon?

Ms. SPEIER. Thank you.

Secretary WORK. I would add two things. One, we have a large number of systems, Congresswoman, that were built in an era, like Admiral Rogers, that was not—the systems were not built to withstand the cyber environment that we are in now. So what keeps me up at night is, can we get through all of our systems and make sure that they do have cyber hardening? Going forward, we are making sure that there are key performance parameters in every system that we have, but we have to go through this risk mitigation on every one of our systems and saying, what is the critical cyber vulnerability? Have we taken care of it? And I would just like to echo, it is manipulation of data, since we rely upon our networks, that really keeps me up at night.

Mr. ROGERS OF ALABAMA. The gentlelady's time is expired.

The Chair now recognizes Chairman Wittman for 5 minutes.

Mr. WITTMAN. Thank you, Mr. Chairman.

Gentlemen, thanks for joining us today.

Secretary Work, I want to begin with getting your perspective on how we address the cyber threat. We have constructed a military that is very adept and capable of addressing kinetic threats, and that is top-to-bottom capability. We have generalists. We have specialists. When enlistees come in, they learn the lessons in training about what to do in that kinetic environment. We have our officers that learn tactics and strategy within that environment. Yet it seems we have a very myopic or piecemeal element with the cyber threat.

Give me your perspective. Shouldn't we have the same top-to-bottom capability and capacity for cyber? Shouldn't our enlisted men and women come in, shouldn't they also get training in the cyber realm? Shouldn't our curriculums at our service academies include very robust and extensive instruction and education within the cyber realm? How do we construct a force that is as capable kinetically as it should be in the cyber realm? And we are far behind, and we need to be catching up. Give me your perspective on how should we do that? Is that valuable to do, and what are you doing to get to that particular point?

Secretary WORK. Congressman, it is very valuable. The first thing is to include—what we call this is improving the cyber hygiene of the entire force, making every single member—Active Duty, civilians, contractors, and Reserves—to understand the cyber threat that we face each day, and to understand the simple actions they can take to improve our security. I think many of the things that you say—in all of our education and our schools, cyber is now an important part of our curriculum. We have red teams that are going out and helping commanders understand where their vulnerabilities are and how they can improve. We have different types of means by which we hold people accountable for like if you have a negligent discharge with a weapon, that is a bad thing. We want everybody to know that a negligent discharge in cyber is almost, I mean, could be as dangerous. So I totally agree with what you are saying, and this is a big, big cyber cultural shift that Admiral Rogers spoke to earlier.

Admiral ROGERS. And I would just echo that is the approach we are taking. This is so foundational to the future for us as a Department in terms of our ability to execute our missions that the Na-

tion is counting on. We have got to do this foundationally across the spectrum. We don't need the same level of training that the dedicated Cyber Mission Force has, but there has got to be a level of basic cyber awareness across our entire force, regardless of rank.

Last comment, this is the one environment in which if we had given you access to a keyboard, you now represent a potential point of vulnerability, and everyone in our Department—that numbers in the millions in terms of the Active Component, contractors, civilians, reservists, Guard—everyone is an operator in this environment.

Mr. WITTMAN. In that realm, that priority also has to be reflected in how resources are dedicated. Give me your perspective: Where are we dedicating resources for things like MILCON [military construction] for cyber, within personnel, within training, within hardware and software? I think it is also reflected not only in what you are doing from a doctrine standpoint, a philosophy standpoint, and training standpoint, but where are you dedicating resources to make sure that you are successfully meeting that objective?

Secretary WORK. Well, when Secretary Carter was the Deputy Secretary filling the job that I fill now, starting around fiscal year 2013, I believe, there was a concerted effort to try to increase the investment in cyber forces. I believe that we are doing very well in this regard. We could always do more. It is budget dependent. But as I said earlier in testimony, Secretary Carter says: Wherever our budget ends up, cyber is going to be a very, very top priority.

The one area where I think we could do better on is in tools. I think we are focused—we had to build the human capital first, which we have been doing very well, but if there is one area where I think we could do better for Admiral Rogers and the team is to invest more money in tools that he would be able to then create better options for the force.

Admiral ROGERS. And I could echo. I think we are doing a very good job with the dedicated Cyber Mission Force in terms of the commitment to bringing it online. Where I think we are going to need to look at over time, as the Secretary said, the things I have raised are tools, situational awareness, persistent training environment, the unified platform, and then asking yourselves over time: Is the manpower piece right? Is the command-and-control structure that we put in place right? And this is part of an ongoing process. What I try to remind people is, look, cyber is an environment in which where we are today is not where we are going to wind up. And we have got to stop focusing on the 100 percent solution up front. We have got to take this in bite-sized chunks and keep moving out.

Mr. WITTMAN. If you could, just for the record, I would love to see a breakdown about what you are proposing in resource allocation now and what your projection is in the future to make sure we are building that capability. And you talked about the time element. Time in this, I think, is critical. So getting your perspective on how you are going to accomplish that, both strategically within the planning sense but also in allocation of resources, is going to be critical.

Secretary WORK. I will take that for the record, sir.

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

Mr. WITTMAN. Thank you.

Mr. ROGERS OF ALABAMA. The gentleman's time is expired.

The Chair now recognize Mr. Ashford for 5 minutes.

Mr. ASHFORD. Thank you, Mr. Chairman.

And many of my questions have been asked and answered. But I want to pick up on something that Admiral Rogers and Mr. Work mentioned a few minutes ago about the government shutdown. You know, and I have been sitting here since February, and I admire everybody on this committee and the witnesses. And I have learned a great deal. I have been here 8 months or whatever.

I am from Nebraska. It is absolutely unfathomable, it is beyond belief, it is incomprehensible that this government or this Congress or anybody would even begin to talk about shutting down the government for whatever political gain they may get. And, you know, we were in the Middle East in February, and at the beginning of the—not the beginning of the ISIS effort, but certainly it was in the beginning stages of our effort to combat ISIS. And we were in Baghdad, and there was discussion at that point about standing up a force to address social media issues. It was at the very, very beginning, beginnings of that, at least in Baghdad, of getting both civilian and military personnel up to speed on what was going on with ISIS and social media. And we are now in October. And I know this is a little bit of a speech, and I apologize. But it seems to me at that time, I came back with the sense of all of the things we talk about in Congress now and all of the discussion about shutting down the government and all of these other issues—I understand this is democracy; we can talk about what we want to talk about. But I kept thinking to myself, why don't we debate and discuss and at least give to the military, every branch of the military, some clear plan and understanding of where we want to go with not only ISIS but in the Middle East, generally?

It seems to me that we are reacting to these various incidents. We are reacting to what the Russians did today because for whatever these existential threats are there; these other threats are there. It seems to me it is incumbent upon us in Congress to clearly indicate to you what we want you to do and where we want you to go because I think that is totally lacking. And this week, with all of the things that went on in the House, I just kept thinking to myself, what is our military thinking about we can't get our house in order? We can't operate. And going back to my service in Nebraska, they look at me like we are nuts. You know, we are sending our military. We are asking them to do almost an impossible task around the globe, and we are bickering about stuff that has nothing to do with giving you the capabilities you need to go forward. So, anyway, I have said enough.

So here is my picking up on your third point about the social media issue, and that is the third thing that keeps you up at night. What is your analysis of where we are—in the next minute and 56 seconds—where we are, Admiral Rogers, where we are with that third element, and how do you see that evolving?

Admiral ROGERS. I think we need to do a better job of contesting ISIL [Islamic State of Iraq and the Levant] in the information dy-

namic. Their ability in the information arena is every bit as important in many ways as their battlefield successes. And we have clearly focused a large piece of our strategy on trying to stop and forestall that battlefield activity level. I think we are going to need to do the same thing in the information dynamic because part of their ability to get out their story, their propaganda, their vision of the world around us, we need to contest that. ISIL is as much an idea in many ways——

Mr. ASHFORD. Right.

Admiral ROGERS [continuing]. As it is a physical presence simplistically on the ground.

Mr. ASHFORD. And how is that going?

Admiral ROGERS. Clearly not where we want it to be. Multiple components across the government ongoing. Don't get me wrong. But I think it is fair to say we have not achieved yet the impact that we think we need to have and certainly the impact that we want to have.

Secretary WORK. And, Congressman, if I could just say that what your opening statement—certainly resonates with Secretary Carter and me. Strategy is all about balancing in ways and means. And when you have no idea what your means are, it is almost impossible to have a good strategy. So as I said earlier today, you know, in the last 6 years, we are in a situation where we think a continuing resolution [CR] is a better deal than a government shutdown, and it is. But it is certainly not something that I as a COO would say I would want to operate under.

In the last 6 years, essentially what we have is a 9-month fiscal year because every first quarter, we are in a CR. And that means that we are limited to do what you told us to do last year, rather than doing the things we need to do this year. It is an incredible situation, and there is no Member of Congress in any House, in any party, that would sit in my job as a COO and say: We can make this work without compromising our national security.

So I am sorry I am on the soapbox, but this is something that we deal with every day. We hope that we won't have a government shutdown. We hope that the CR will be taken care of in a very quick manner.

Mr. ASHFORD. Right. My time is up, but thank you very much. Thank you, Mr. Chairman.

Mr. ROGERS OF ALABAMA. I thank the gentleman.

The Chair now recognizes Ms. McSally for 5 minutes.

Ms. MCSALLY. Thank you, Mr. Chairman.

Thank you, gentlemen.

And now that you are on the topic, I want to make sure I am on the record that I, after serving 26 years in uniform and seeing government shutdowns and continuing resolutions and the impact that that has on our ability to do our mission, I have been strongly advocating against shutting down the government; strongly advocating for us doing our job and actually passing appropriations bills so that you guys can plan, you can strategize, you can execute the mission. And I would urge all of my colleagues, if you want to keep the government open, you need to vote to keep the government open. And that would be my urge to them today. Those of us who understand what that means are going to do that, but we would

appreciate a large number of my colleagues actually showing some courage in joining us.

Anyway, on to the issues at hand. Prior to running for Congress, I was a professor at the George C. Marshall Center, one of our defense security centers. And one of the last courses that I participated in was a Senior Executive Seminar related to cybersecurity, cyberterrorism.

And so, in your strategy, you talk about building and maintaining robust alliances, partnerships. Obviously, this is, you know, a global domain, and so they are now starting a—one of my colleagues, Phil Lark, retired Marine colonel, is starting a program on cybersecurity studies or he is leading that effort.

And so I am wondering if you could speak to how the defense security centers fit in with this strategy; how you feel as far as resources in order to use tools like these security centers, like the Marshall Center, to execute that strategy; and whether you need new authorities or additional resources in that venue.

Secretary WORK. Well, first of all, these different centers are very vital. Part of our strategy, regardless of what the level of resources are, Congresswoman, is partnerships.

Ms. MCSALLY. Yeah.

Secretary WORK. And establishing strong partnerships, and as Admiral Rogers and Terry have said, this is a collaborative environment that we all face the same threats and need to operate together.

Ms. MCSALLY. Right.

Secretary WORK. So I don't know if there are any authorities that Mike would ask to help us work more deeply with our partners, but I know that we are doing so very aggressively.

Admiral ROGERS. I would say——

Ms. MCSALLY. Resources as well, yeah.

Admiral ROGERS. Right. It hasn't been an authorities issue as much. And the case specifically of the Marshall Center, General Breedlove, in fact, has asked both I and the Department, you know, for assistance, said: Hey, this is important to me; I think it will generate good outcomes for us in Europe——

Ms. MCSALLY. Right.

Admiral ROGERS [continuing]. As we are trying and understand the broader cyber environment. So I have committed to General Breedlove: Hey, look, I will be there to provide expertise to help because that is what I can bring, not necessarily money.

We are working—I don't think either of us off the top of our heads know the specifics, other than the fact that we have committed to moving forward on that. I know it is ongoing.

Ms. MCSALLY. Yeah, and I will tell you, having been there—and sometimes we have senior officials from 45 different countries—this is not a technical course. It is more of an awareness of best practices, policy issues, especially for some of our less capable partners. They are not going to ever have a Cyber Command like we do, but if we can raise their game up a bit and we can have better collaboration and coordination for strategic understanding and best practices, how to quickly alert and respond and working with each other intelwise, threatwise, I think it goes a long way. I mean, I was very impressed with the capabilities that we have there. And

I would think it is a little bit of an investment for potentially huge strategic outcomes.

Secretary WORK. We agree with you completely.

Mr. HALVORSEN. I will just say some of that work is related. Mike will be doing some things, but over the next months, we will be in NATO working to do exactly that with some of our partners, raising their cyber basics.

Ms. MCSALLY. Right.

Mr. HALVORSEN. We will be in Bulgaria doing the same thing, and some of that is a result of some of the arrangements that were worked frequently from the Marshall Center.

Ms. MCSALLY. Yeah. Great.

Mr. HALVORSEN. That is paying back some good dividends.

Ms. MCSALLY. Excellent. I look forward to working with you in the future if you have any other additional requests related to that with the firsthand experience that I have, so not just the Marshall Center but the other defense centers, obviously, because this is a global issue.

So I thank you, gentlemen. I appreciate it.

Mr. Chairman, I yield back.

Mr. ROGERS OF ALABAMA. I thank the gentlelady.

The Chair now recognizes Ms. Duckworth for 5 minutes.

Ms. DUCKWORTH. Thank you, Mr. Chairman.

Gentlemen, I am very interested in looking at cyber vulnerabilities in our critical infrastructure. I would love to drill down more specifically to our bases and installations that support core warfighting functions. I feel that they face similar threats.

Our installations are tied into local grids, rely on sewage and water from the surrounding areas, so there is always potential for impact for those basic life services on the base. Certainly continuity of operations is critical for DOD, just as it is for our civilian infrastructure.

Admiral, I would like for you to sort of address this, and I am going to give you an example that I found deeply, deeply disturbing. I took a tour of a contractor that—a wonderful company that works in smart grid technology. And as part of this tour of this facility, small business, they were very proud to show me what they were doing. They had won a contract at one of our facilities, one of our bases. Actually, the base where a major—I won't say which base it is because this is not a secret room, but it was the home for a major maneuver division in the Army. And from another State where I was, I watched them turning off the lights at that base.

And then when I asked the person who was operating the computer, who was turning the lights on and off at this base, I said: "Do you have a secret clearance?"

They said, "No."

I said: "Do you, as the company, have anybody with a secret clearance?"

"Yes, the chief engineer does."

But this is an unsecure room. People in the business were coming in and out. And they were very—I mean, amazing technology that is going to help us save tons of money when it comes to environmental costs and energy efficiency and all those good things as

a Democrat I love. But I was deeply, deeply concerned that I was sitting there watching them turn the lights on and off on a major road on a major installation of a major maneuver division command in the Army.

Admiral, if you could speak a little bit to perhaps what you are doing to both coordinate with Installations Command for each of the different branches, whether it is the Army's Installation Management Command, the Marine Corps' Installations Command, and also local civilian infrastructure as well. And, by the way, this base is outside of a major metropolitan city. It is not one of the Army bases that is out in the middle of nowhere. I spent a lot of time at those myself, but I was deeply concerned.

Admiral ROGERS. So we share your concern. The services and installation and their respective installation commands are working with each individual installation. I had been an installation commander myself in the course of my career, so I have experienced this as a commander. When you are so dependent in some ways on infrastructure and capability that is outside of your immediate span and control and yet it directly derives your ability to execute your mission, it is one of the reasons why collectively in the Department, we ask ourselves: So what are the capabilities we need to bring on the installation, if you will, to put redundancy and backups in so we have a level of control?

We are working our way through this. The challenge I think we find is, again, it goes just the scope of the problem sets out there, just the infrastructure that we count on as a Department, that just the broad swath of it, the size and the age of it in many ways as we are trying to collectively work our way through this. This is a problem set that is going to take us years to work our way through. I don't think there is any doubt about that.

Ms. DUCKWORTH. Do you have a liaison from Cyber Command that sits at installation command for each of the branches of service?

Admiral ROGERS. No. What I do is I work through my service components who partner with their installation command. So, for example, in my last job where I was the Navy's cyber individual reporting to U.S. Cyber Command, I was working directly with the Navy's Installations Command as to what we were doing in naval installations, you know, around the world for us, and we still do that now.

Ms. DUCKWORTH. Is there any policy that looks at—and one of the great things about this committee is this is a very bipartisan committee. And I want to applaud our chairman for his continuing work on acquisition reform.

But one of my concerns with acquisition reform is these contractors and sub-subcontractors. Huawei North American Regional headquarters is actually in my district. And I have concern that we are talking about service subcontractors that are several layers down, and we are not inspecting them. I mean, there was nobody inspecting this contractor and making sure that they were—I mean, that they had, you know, secured the facilities and their computers and the devices that are in the hands of people who are actually turning on and off the lights at a major military base.

Admiral ROGERS. Right. So we have taken the Huawei issue specifically for action. We will provide feedback on that. This, I share your concern, ma'am. This is something we are going to have to just work our way through.

Ms. DUCKWORTH. What do you specifically—do you have plans in place? Are you writing policy? What are you doing specifically to address this particular issue?

Admiral ROGERS. I apologize——

Mr. HALVORSEN. Mike, let me take that one.

Admiral ROGERS. Yeah.

Mr. HALVORSEN. There is policy in place. We are looking at all of the installations and, frankly, grading them and looking for where are the priorities.

But as Mike said, this is a priority issue. There is a vast number of, you know, installations. Very frankly, the control systems for power and water when they were built, there was no consideration of cyber, so now we have to go back and fix that.

We have a list of those priorities. We are prioritizing on those bases that have more strategic assets first, which I think is smart, and we will keep going down that list to fix those issues. But there is a priority list. We have new language required in the FAR [Federal Acquistion Regulation] for all levels of contractors now to meet certain requirements about the security control systems, and that is in place.

Ms. DUCKWORTH. Can I have a copy of your priorities list and that new language for contractors? Is that available for Members of Congress?

Mr. HALVORSEN. We will certainly take that for the record. I am sure it is, and we will figure out how to get it to you.

[The information referred to can be found in the Appendix on page 74.]

Ms. DUCKWORTH. Thank you.

I yield back, Mr. Chairman.

Mr. ROGERS OF ALABAMA. The Chair now recognizes the gentleman from Arizona, Mr. Franks, for 5 minutes.

Mr. FRANKS. Well, thank you, Mr. Chairman.

Admiral Rogers, I appreciate people like you that put yourself at risk and assiduously try to do everything you can to protect the homeland and the future generations. So, on behalf of my children, thank you.

Admiral ROGERS. Thank you, sir.

Mr. FRANKS. I am going to paraphrase here, but in recent press briefings at the Wilson Center, you said that what keeps you up at night—and I know you have been asked that question several times today—are threats to critical infrastructure and that you have been observing nation-states spending a lot of time within the power structure of the United States. And as you know better than perhaps anyone, the Department of Defense relies upon the electric grid for 99 percent of its electricity needs, without which even the Department's position is that it cannot effect its mission.

And, of course, there are 320 million Americans that also depend upon it pretty significantly for everyday survival. And a widespread collapse of the electric grid, of course, would lead to gross societal collapse.

So wearing your CYBERCOM hat, how protected is our electric grid from, number one, cyberattacks and lesser discussed attacks that could come from geomagnetic disturbance or electromagnetic pulse? And do you find industry to be a willing partner in helping to secure the grid? And what have you been tasked with or coordinated with or asked to do from the Department of Homeland Security or the FERC, Federal Energy Regulatory Commission, in regards to hardening the electric grid and protecting it and just giving us your best military advice? A lot of questions here, I am sorry. What do you think needs to be accomplished to robustly harden our electric grid against these stated threats?

Admiral ROGERS. Let me try to do them backwards to forwards.

Remember, DOD does not physically act on private sector networks. I am not responsible for hardening them.

Mr. FRANKS. That is true, but without them, you will certainly maybe revisit that.

Admiral ROGERS. Right. My only point is, your question specifically, though, is, what are you doing as—well, that is not Cyber Command's role. What we do is we partner with DHS in their role. I try to make sure that, again, because one of the missions you heard the Secretary talk about in the very beginning, where there is an expectation that DOD needs to be ready to respond if the President decides that we have to respond to a cyber event of significant consequence, a power scenario is definitely one of the things that we talk about.

So we partner with DHS. We partner with the segment—for example, we do a Cyber Guard annual exercise. I had two different power sector segments from two different parts of the United States that participated in this exercise. That was one of the scenarios we walked our way through.

In terms of the grid, if you will, vulnerability, I would argue it is pretty broad. If you look in the eastern part of the United States, the grid is operating on the margin already just between capacity and demand.

The other point I try to make, particularly in the eastern part of the United States, is we need to think more than just the U.S. Our grid in the east in particular is so tied into our Canadian counterparts for hydroelectric and other power generation. Capacity on their side of the border often is flowing south to meet our basic needs.

The other challenge I find in the power sector is—and they are quick to remind me of this—is their business model: "A, Admiral, we are a regulated industry. The only way for us to generate revenue is through rates. Those are governed. I just can't universally say I am going to upcharge this to generate a $5 billion capital fund that I can use to invest in basic infrastructure." So each of the utilities, if you will, within the sector is trying to work their way through it.

Mr. FRANKS. Well, now, I appreciate that.

I guess one of things over the years in dealing with this issue that has occurred to me is that what you just said—and you are absolutely correct; I mean, you know, this is not your responsibility to tell the private sector what to do with the grid. But then the private sector, when we talk to them about hardening the grid for na-

tional security purposes, they say that is the national defense apparatus' job. And, in the meantime, this, what could be a profound threat, given the fact that all of our other security, our other critical infrastructures rely heavily upon the grid, it walks the 13th floor of congressional debate, and no one addresses it.

And, of course, you know, there is always a moment in the life of every problem when it is big enough to be seen and still small enough to be addressed. And I think we live in that window. So I certainly don't offer you any advice. Just the question I hope lingers in our minds is, are we doing what is relevant to protect the national security on this particular threat because certainly a loss of the grid would be the ultimate cybersecurity issue? I mean, you know, if you can't turn those computers on, you can't do really much else.

Again, there is no arrogance in my comments, Admiral. I think that you are doing a great job, and I hope you will consider this as much as possible.

Admiral ROGERS. Certainly.

Mr. FRANKS. Thank you.

Mr. ROGERS OF ALABAMA. I thank the gentleman for yielding back.

All of our members have completed their questions.

I want to thank the witnesses for their time and preparation for this hearing. I know it takes a lot to get ready for these and your time here today, but it has been very beneficial to us.

And, with that, we are adjourned.

[Whereupon, at 12:15 p.m., the committee was adjourned.]

A P P E N D I X

SEPTEMBER 30, 2015

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

SEPTEMBER 30, 2015

AS PREPARED – EMBARGOED UNTIL DELIVERY

DEPUTY SECRETARY OF DEFENSE ROBERT O. WORK
OPENING STATEMENT BEFORE THE HOUSE ARMED SERVICES COMMITTEE
WEDNESDAY, SEPTEMBER 30, 2015

Chairman Thornberry, Ranking Member Smith, and members of the Committee, thank you for inviting me to discuss Department of Defense (DoD) efforts in cyberspace. The Department of Defense is currently implementing the DoD Cyber Strategy, published in April 2015, to improve our Nation's capabilities to conduct cyberspace operations and deter potential adversaries from engaging in malicious cyber activity against the United States.

Cybersecurity Risks to DoD Networks and Infrastructure

Cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting government and business activities, and imposing significant costs to the U.S. economy. State and non-state actors are conducting cyber operations, expanding their capabilities and targeting the public and private networks of the United States, our allies, and partners. These cyber threats continue to increase and evolve, posing greater risks to the networks and systems of the Department of Defense, our Nation's critical infrastructure, and U.S. companies and interests globally.

External actors probe and scan DoD networks for vulnerabilities millions of times each day and foreign intelligence agencies continually attempt to infiltrate DoD networks. Unfortunately, some incursions – by both state and non-state entities – have succeeded. The intrusion into the Office of Personnel Management security clearance systems compromised the personal information of millions of U.S. government employees, their families, and their associates. In recent years, there have been several notable cyber intrusions on DoD networks, to include the Joint Staff intrusion, and interception of DoD data not residing on DoD networks, e.g. the TRANSCOM and OPM intrusions.

Cyberattacks also pose a serious risk to networks and systems of critical infrastructure. The Department of Defense relies on U.S. critical infrastructure, as well as the critical infrastructure of our international partners, to perform its current and future missions. Intrusions into that infrastructure may provide access for malicious cyber actors who wish to disrupt critical systems in a time of crisis. Because of the potentially severe consequences, DoD is working with our partners in the interagency, private sector, and international community to ensure these systems are better protected and more resilient.

At DoD we are also increasingly concerned about the cyber threat to companies in our Defense Industrial Base. We have seen an unacceptable loss of intellectual property and sensitive DoD information that resides on or transits Defense Industrial Base unclassified systems. This loss of key intellectual property has the potential to damage our national security as well as impede economic growth by eroding U.S. technical superiority.

Cyber Threats

Malicious actors are also targeting U.S. companies. At the end of last year, North Korean actors attacked Sony Pictures Entertainment in the most destructive cyberattack against a U.S. company to date. North Korea destroyed many of Sony's computer systems, released personal and proprietary information on the Internet, and subsequently threatened physical violence in retaliation for releasing a film of which the regime disapproves. The President stated that the United States will pursue an appropriate response to the incident – which he said would be reserved for a time, place, and manner of his choosing. To date the United States has publicly attributed the attack to the North Korean government, and in January 2015 the President signed new sanctions Executive Order in response to North Korea's provocative, destabilizing, and repressive actions and policies.

North Korea isn't our only adversary that has engaged in cyberattacks. Iran has also conducted cyberattacks against private sector targets to support its economic and foreign policy objectives, at times concurrent with political crises. Iranian actors have been implicated in the 2012-13 DDOS attacks against US financial institutions and in the February 2014 cyberattack on the Las Vegas Sands casino company. Iran very likely views its cyber program as one of many tools for carrying out asymmetric but proportional retaliation against political foes, as well as a sophisticated means of collecting intelligence.

Chinese cyber espionage continues to target a broad spectrum of US interests, ranging from national security information to sensitive economic data and US intellectual property. Although China is an advanced cyber actor in terms of capabilities, Chinese hackers are often able to gain access to their targets without having to resort to using advanced capabilities. Improved US cybersecurity would complicate Chinese cyber espionage activities by addressing the less sophisticated threats, and raising the cost and risk if China persists.

Russia's Ministry of Defense is establishing its own cyber command, which—according to senior Russian military officials—will be responsible for conducting offensive cyber activities, including propaganda operations and inserting malware into enemy command and control systems. Russia's armed forces are also establishing a specialized branch for computer network operations. Computer security studies assert that Russian cyber actors are developing means to remotely access industrial control systems (ICS) used to manage critical infrastructures. Unknown Russian actors successfully compromised the product supply chains of at least three ICS vendors so that customers downloaded malicious software (malware) designed to facilitate exploitation directly from the vendors' websites along with legitimate software updates, according to private sector cyber security experts.

Non-state actors also continue to be very active in conducting malicious cyber activities. Terrorist groups, including ISIL, experiment with hacking which could serve as the foundation for developing more advanced capabilities. Terrorist sympathizers conduct low level cyberattacks on behalf of terrorist groups and attract attention of the media, which might exaggerate the capabilities and threat posed by these actors. With respect to ISIL, since last summer, the group began executing a highly strategic social media campaign using a diverse array of platforms and thousands of online supporters around the globe.

Profit motivated cyber criminals continue to successfully compromise the networks of retail businesses and financial institutions in order to collect financial information, biographical data, home addresses, email addresses, and medical records that serve as the building blocks to criminal operations that facilitate identity theft and fraud. These criminals rely on loosely networked online marketplaces, often referred to as the cyber underground, that provide a forum for the merchandising of illicit tools, vulnerabilities, services, infrastructure, stolen personal identifying information, and financial data.

The combination of these diverse cyber threats results in a complex and challenging threat environment. To conduct a disruptive or destructive cyber operation against a military or industrial control system requires expertise, but a potential adversary need not spend millions of dollars to develop an offensive capability. A nation-state, non-state group, or individual actor can purchase destructive malware and other capabilities through the online marketplaces created by cyber criminals, or through other black markets. As cyber capabilities become more readily available over time, the Department of Defense assesses that state and non-state actors will continue to seek and develop malicious cyber capabilities to use against U.S. interests.

DoD's Cyber Strategy

In response to the growing cybersecurity threats and to guide the Department's efforts to defend our Nation against cyberattacks of significant consequence, we developed the 2015 DoD Cyber Strategy. Our new cyber strategy, the Department's second, guides the development of DoD's cyber forces and strengthens our cybersecurity and cyber deterrence posture.

The strategy focuses on building cyber capabilities and organizations for DoD's three primary cyber missions: to defend DoD networks, systems, and information; defend the Nation against cyberattacks of significant consequence; and provide cyber support to operational and contingency plans. To accomplish these missions, the strategy sets five strategic goals:

1. Build and maintain ready forces and capabilities to conduct cyberspace operations;
2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;
3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages; and,
5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

In support of these goals, we are building the Cyber Mission Force, training it to conduct full-spectrum cyberspace operations, and equipping it with the tools and infrastructure it needs to succeed. This force is composed of four types of teams: 68 Cyber Protection Teams to defend priority DoD networks and systems against significant threats; 13 National Mission Teams to defend the United States and its interests against cyberattacks of significant consequence; 27 Combat Mission Teams to provide support to Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations; and 25 Support Teams to provide analytic and planning support to the National Mission and Combat Mission

Teams. Once fully manned, trained, and equipped in Fiscal Year 2018, these 133 teams will execute DoD's three primary missions with nearly 6,200 military and civilian personnel. However, many of these developing teams are already adding significant cyberspace capabilities to DoD now, as they actively conduct critical ongoing missions while building their operational capacity.

As we continue to strengthen the Cyber Mission Force, we recognize the need to incorporate the strengths and skills inherent within our Reserve and National Guard forces. Each Service, therefore, has developed Reserve Component integration strategies that provide a total force cyber capability and leverage the Reserve and National Guard strengths from their experience in the private sector. Up to 2,000 Reserve and National Guard personnel will also support the Cyber Mission Force by allowing DoD to surge cyber forces in a crisis.

As Secretary Carter has stated, the development of a cadre of cyber experts – both in and out of uniform -- is essential to the future effectiveness of U.S. cyber capabilities, and we are committed to ensuring that the workforce for the cyber domain is world class. To that end, we must develop and retain a workforce of highly skilled cybersecurity specialists with a range of operational and intelligence skill sets. This cyber workforce must include the most talented experts in both the uniformed and civilian workforce, as well as a close partnership with the private sector.

The Department is taking a hard look at barriers and challenges to recruitment, retention, employment, compensation, promotion, and career progression for DoD's cyberspace workforce. We are developing recommendations that could provide the Department, USCYBERCOM, and the Service Cyber Components with the workforce management authorities and flexibilities that would strongly enable the successful execution of their cyberspace missions and responsibilities. Section 1104 of the National Defense Authorization Act currently under conference is a vitally important step to help DoD attract, hire, and retain a world class cyber workforce.

The Department is aggressively implementing our Cyber Strategy across all three missions and five goals. We have developed detailed outcomes, milestones, timelines, and metrics for each objective in the DoD Cyber Strategy. Additionally, in accordance with Section 932 of the Fiscal Year 2014 National Defense Authorization Act, we have established a cross-functional, interdepartmental team to support the Principal Cyber Advisor to oversee its execution, coordinating with all DoD stakeholders, and proactively addressing potential obstacles. As we implement the strategy, we are also taking a number of steps to improve budgeting and accounting for the Cyber Mission Force across the Department and appreciate your continued support on these issues.

Deterrence

Deterrence is a key mission for the Cyber Mission Force in the new DoD Cyber Strategy. Deterrence is a function of perception; it works by convincing a potential adversary that the costs of conducting an attack outweigh any potential benefits. DoD needs the ability to deter or prevent disruptive and destructive cyberattacks, preempt an imminent cyberattack, halt an ongoing cyberattack, and respond to cyberattacks. To do that, DoD must develop on-the-shelf

capabilities that could have the ability to affect an adversary's behavior by shaping the environment, controlling escalation, and imposing costs. Additionally, we must strengthen our overall resilience posture so that DoD networks and systems can continue to operate even while under attack. Denial, resilience, and response are key components to a holistic deterrence strategy, expanding well past just the cyber domain.

Denial

First, as a part of our strategy we must increase our denial capabilities to tilt any adversaries' cost-benefit analysis in our favor. To deny an attack from adversely affecting our military missions, we must first defend our own information, networks, data, and systems. We are focused on two aspects of denial: strengthening DoD's cybersecurity; and defending the nation against cyberattacks of significant consequence.

As Secretary Carter has said, the first of our three missions is to defend our own information networks, data, and systems. Without secure systems, we cannot do any of our missions. So, the DoD is working to implement best in class technical solutions. We are standardizing our boundary defenses under the Joint Information Environment, providing linkages from our intelligence capabilities for early warning, while including state of the art commercial technologies to create comprehensive capabilities across the cyber kill chain and enable dependable mission execution in the face of highly capable cyber adversaries. As a foundational element to achieve this, we are globally deploying the Joint Regional Security Stacks (JRSS) to significantly reduce the avenues of attack into our unclassified and classified networks, support advanced threat analytics and improve responsiveness to attack. This will allow increased security and visibility, ensuring that commanders can see and respond to threats in order to determine risk to mission. The Department has also embarked on a new scorecard system that will hold commanders accountable for hardening and protecting their endpoints and critical systems. However, we also recognize that technical upgrades and organizational changes are only part of the solution when it comes to effective cybersecurity. Nearly all successful network exploitations can be traced to one or more human errors, so raising the level of individual human performance in cybersecurity will provide us with tremendous leverage in defending DoD networks. Accordingly, we are closely considering how we can transform DoD cybersecurity culture for the long term by improving human performance and accountability.

The President has directed DoD to work in partnership with other agencies to be prepared to blunt and stop the most dangerous attacks from succeeding. There may be times when the President or the Secretary of Defense may direct DoD and others to conduct a defensive cyber operation to stop a cyberattack from impacting our national interests. This is DoD's mission: to defend the nation against cyberattacks of significant consequence – which may include loss of life, destruction of property, or significant foreign and economic policy consequences. It means building and maintaining capabilities to prevent or stop a potential cyberattack from achieving its effect.

This is a challenging mission. It requires high-end capabilities and highly trained teams. We are building our Cyber National Mission Force and deepening our partnerships with law enforcement and the intelligence community to do it.

Resilience

Improving DoD's resilience will reduce the incentive for adversaries to attack us through cyberspace and protect our ability to execute missions in a degraded cyber environment. This means normalizing cybersecurity as part of our mission assurance efforts, building redundancy wherever our systems are vulnerable, and training constantly to operate in a contested cyber environment. To deter our adversaries, they must see that cyber-attacks will not provide them with significant operational advantage.

DoD also relies on civilian and international infrastructure to execute its missions. We partner with the interagency, the private sector, and other countries to ensure the cybersecurity and resilience of the critical infrastructure on which we all rely. Organizations across the country are beginning to recognize the importance of resilient systems. IT companies and critical infrastructure owners and operators are driving market supply and demand towards more secure IT products and services, and that is great news.

Response

Finally, in the event of a potential cyberattack on U.S. interests, the United States must be able to respond through cyber or non-cyber means to impose costs on a potential adversary. Throughout this Administration, we have made clear that the United States will respond to cyberattacks in a time, manner, and place of our choosing.

Therefore a key objective of the DoD Cyber Strategy is to develop cyber options to hold an aggressor at risk in cyberspace if required. To support our deterrence posture, DoD is investing significantly in our Cyber Mission Force, including robust intelligence and warning capabilities to better identify malicious actors' tactics, techniques, and procedures in order to improve attribution in cyberspace. These attribution capabilities have increased significantly in recent years, and we continue to work closely with the intelligence and law enforcement communities to maintain and continue to improve them through intelligence collection and forensics.

But in many instances, non-cyber capabilities may provide a more appropriate or effective response. The Administration reviews the whole range of options, such as diplomatic engagement, network defense and law enforcement measures, economic or financial sanctions, or even the use of kinetic capabilities. Responses will be selected on a case by case basis, and be conducted consistent with law.

Building Strong Partnerships

Successfully executing our missions in cyberspace requires a whole-of-government and whole-of-nation approach. DoD continues to work with our partners in other federal Departments and agencies, the private sector, and countries around the world to address the shared challenges we face. We work particularly closely with our partners in the Department of Homeland Security and Department of Justice to ensure collaboration in cyber operations and information sharing

across the federal government, and we have seen tremendous advancement in our ability to work as a single, unified team.

We also work closely with our partners and allies to ensure that we maintain a strong collective defense against cyber threats. Through cooperation, shared warning, capacity building, and joint training activities, international engagement provides opportunities for an exchange of information and ideas to strengthen our cybersecurity as well as that of our allies and partners. Our partners are increasingly prioritizing cybersecurity as a key national security issue, creating opportunities and new areas for cooperation. We cooperate with, and assist, a wide range of partners.

Additionally, Secretary Carter has placed a particular emphasis on partnering with the private sector. We need to be more creative in finding ways to leverage the private sector's unique capabilities and innovative technologies. The Department does not have all the answers, and working with industry will be critical to we remain at the cutting edge of technology to protect our nation. We are examining ways to expand our collaboration with industry and are developing incentives and pathways to bring more cyber expertise into the Department.

Finally, our relationship with Congress is absolutely critical. As the President has said many times, Congressional action is vital to addressing cyber threats. I appreciate the support provided for DoD cyber activities throughout the 2016 National Defense Authorization Act. And, I encourage continued efforts to pass legislation on cybersecurity information sharing, data breach notification, and law enforcement provisions related to cybersecurity, which were included in the President's legislative proposal submitted earlier this year.

Conclusion

It is my job is to make sure that our strategy is effectively implemented across the Department, and ensure that DoD is moving forward coherently and comprehensively in performing its assigned cybersecurity roles. The American people expect us to defend the country against cyber threats of significant consequence, and I look forward to working with this Committee and the Congress to ensure we continue to take every step necessary to confront the substantial cybersecurity risks we face. Thank you, again, for the attention you are giving to this urgent matter. I look forward to your questions.

Robert O. Work
Deputy Secretary of Defense

Robert O. Work was confirmed as the 32nd Deputy Secretary of Defense on April 30, 2014.

Mr. Work most recently served as Chief Executive Officer of the Center for a New American Security (CNAS). From 2009 to 2013, Mr. Work served as the Undersecretary of the Navy. In this capacity, he was the Deputy and Principal Assistant to the Secretary of the Navy and acted with full authority of the Secretary in the day-to-day management of the Department of the Navy.

In 2008, Mr. Work served on President-elect Barack Obama's Department of Defense Transition Team as leader of the Department of the Navy issues team. He also worked on the defense policy, acquisition, and budget teams.

In 2002, Mr. Work joined the Center for Strategic and Budgetary Assessments (CSBA), first as the Senior Fellow for Maritime Affairs, and later as the Vice President for Strategic Studies. In these positions, he focused on defense strategy and programs, revolutions in war, Department of Defense transformation, and maritime affairs.

Mr. Work was also an adjunct professor at George Washington University, where he taught defense analysis and roles and missions of the armed forces.

Mr. Work was a distinguished graduate of the Naval Reserve Officers Training Course at the University of Illinois, and was commissioned a second lieutenant in the U.S. Marine Corps in August 1974. During his 27-year military career, he held a wide range of command, leadership, and management positions. He commanded an artillery battery and a battalion, and was the base commander at Camp Fuji, Japan. His last assignment was as Military Assistant and Senior Aide to the Honorable Richard Danzig, 7lst secretary of the Navy.

Mr. Work earned a Bachelor of Science degree in Biology from the University of Illinois; a Master of Science in Systems Management from the University of Southern California; a Master of Science in Space System Operations from the Naval Postgraduate School; and a Master in International Public Policy from the Johns Hopkins School of Advanced International Studies. He is a member of the International Institute for Strategic Studies (IISS). His military and civilian awards include the Legion of Merit, Meritorious Service Medal, Defense Meritorious Service Medal, and the Navy Distinguished Civilian Service Award.

Terry Halvorsen
Chief Information Officer

Terry Halvorsen assumed the duties as the Department of Defense Chief Information Officer effective March 8, 2015. He previously served as the Acting Department of Defense Chief Information Officer. Prior to that, he was the Department of the Navy Chief Information Officer.

As DoD CIO, Mr. Halvorsen is the principal advisor to the Secretary of Defense for Information Management / Information Technology and Information Assurance as well as non-intelligence space systems; critical satellite communications, navigation, and timing programs; spectrum; and telecommunications. He provides strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology-based capabilities required to support the broad set of Department missions.

Before serving as the Department of the Navy CIO, Mr. Halvorsen was the deputy commander, Navy Cyber Forces. He began serving in that position in January 2010 as part of the Navy Cyber reorganization. Previous to that, Mr. Halvorsen served as the Deputy Commander, Naval Network Warfare Command. He was responsible for providing leadership for over 16,000 military and civilian personnel and supporting over 300 ships and approximately 800,000 globally dispersed computer network users. In this position he was responsible for the business performance of Navy network operations, space operations, information operations and knowledge management.

Mr. Halvorsen served as an Army intelligence officer in a variety of assignments, including Operations Just Cause and Desert Storm. He holds a bachelor's degree in history from Widener University, and a master's degree in educational technology from the University of West Florida. He is a Rotary International Paul Harris Fellow and an Excellence in Government Leadership Fellow.

STATEMENT OF

ADMIRAL MICHAEL S. ROGERS

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

30 SEPTEMBER 2015

Chairman Thornberry, Ranking Member Smith, and distinguished members of the Committee, thank you for the opportunity to speak to you today about the implementation of our military strategy in cyberspace. It is an honor to appear today beside Deputy Secretary of Defense Robert Work as well. Let me also mention the great and justified pride I take in the privilege of speaking on behalf of the men and women of United States Cyber Command (USCYBERCOM) and the vital work they undertake to defend our nation. Their efforts guided by the new DoD Cyber Strategy and supported by the indispensable contributions of the National Security Agency (which I also head), are improving our cyber security with the Department of Defense (DoD) and our ability to generate a greater range of options with cyber to support policy makers and operational commands. All of this helps keep our fellow citizens safe and advance our national interest overseas.

In line with the DoD Cyber Strategy, USCYBERCOM and its components perform three primary missions. First, we are responsible for securing, operating, and defending Department of Defense systems and networks, which are fundamental to the execution of all Department of Defense missions. Second, the Department of Defense and the nation rely on us to build ready cyber forces and to prepare to conduct cyber operations to deter or defeat strategic threats to the nation. Third, we work with the Combatant Commands to integrate cyber operations into broader military missions. Our military is already engaged in cyberspace. Potential adversaries scan DoD networks for vulnerabilities millions of times daily. As we have repeatedly seen, a vulnerability in one place can be a weakness across an entire network and systems built as "administrative" networks are now on the front lines of our operations. This reality has serious implications for our nation's security, as well as for our military.

We are at a strategic inflection point where the great promise and opportunity offered by cyberspace innovation has also made it easier for potential adversaries to find vulnerabilities that they can use to threaten us. The DoD Cyber Strategy seeks to generate and align a multi-faceted effort within the Department against an unprecedented and growing challenge. In announcing the Strategy last April, Secretary Carter noted that threats are proliferating and diversifying. Digital tools in cyberspace give adversaries cheap and ready means of doing something that until recently only one or two states could afford to do: that is, to reach beyond the battlefield capabilities of the U.S. military. They have demonstrated the capacity to hold "at risk" our military and even civilian infrastructure. In lay terms, that means that decades of military investment is now imperiled, because as Secretary Carter says, our forces depend on the functioning of our military networks and combat systems, without which they, and we, are far less effective in all domains.

How do we know this, and what does it mean? Recent events have made this trend clear, and we know it because of our intelligence analysis. We have recently seen Russian and Chinese-sponsored intrusions in U.S. information systems – penetrations that were designed to (and in some cases did) gain persistent presence in the targeted networks. And of course, no one missed the North Korean attack on Sony Pictures Entertainment last year, when a state turned its cyber capabilities against a private U.S. corporation, stealing its intellectual property, damaging its property, disrupting its operations, invading the privacy of its employees and affiliates, and threatening its customers and suppliers. We have also observed that energy firms and public utilities in many nations (including the United States) have had their networks compromised by state cyber actors.

Secretary Carter has also noted the risk of miscalculation and escalation resulting from malicious cyber actions, and Deputy Secretary of Defense Work recently told an audience in London that conventional deterrence is eroding to a worrisome degree. Addressing that risk in the cyberspace domain is the point of the DoD Cyber Strategy – to defend, and show we can defend, and thus to preserve the effectiveness of our "traditional" instruments of national power. Let me illustrate one important way in which we are implementing this strategy, with a quick historical detour for context.

Preparing to Respond

Our military has found ways to adapt to new technologies, strategies, and tactics in the past. For instance, we exercised the U.S Army in Louisiana in April 1940 and learned that the sort of trench warfare that had dominated battlefields in the last World War had subsequently been overtaken by events—or more precisely, by tanks, dive bombers, and mobile infantry, all coordinated by radio. The Fall of France to the German *blitzkrieg* barely two months later showed what happened to nations that failed to heed recent advances in military art – a German force with fewer tanks and guns routed the French and British armies in just six weeks. Our War Department incorporated this lesson and returned to Louisiana in the summer of 1941 to test its new concepts. This time the U.S. Army, augmented by National Guard formations, ran two maneuvers, ultimately involving half a million troops. The first phase showed that the *blitzkrieg* could indeed be stopped, and the second showed that our Army could mount a *blitzkrieg* of its own. Those extended exercises gave us invaluable experience, prompting changes to doctrine, weapons, and concepts.

The Louisiana Maneuvers could not foreordain victory in World War II, of course, but they helped prepare our military for a new and global conflict by giving officers and soldiers the opportunity and latitude to experiment and even fail at employing new weapons, tactics, and modes of operation. Those maneuvers also drove home the point of the experimentation: to practice being agile, not just defending but being ready and able to go on the offensive and hit back, taking the fight to the opponent. That is just the sort of experimentation we must continue doing today. Then-Army Chief of Staff George C. Marshall was questioned about the expense of such large maneuvers by a Senator who also pointed out that the exercises had witnessed a lot of mistakes by the forces involved. Marshall characteristically responded respectfully but firmly: "I want the mistake [made] down in Louisiana, not in Europe." Discovery learning in the midst of real-world operations, as the British and French experienced in 1940, can be disastrous. The DoD Cyber Strategy is intended to enable us to learn in peacetime how to succeed in cyberspace operations under all conditions. Today we have "lessons learned" instead of mistakes, of course, and we are doing so in Virginia, where last summer we staged for the fourth time our large, annual exercise that we call CYBER GUARD.

We inaugurated the CYBER GUARD exercise series to test the "whole of nation" response to a major cyber incident affecting the DoDIN and U.S. critical infrastructure. USCYBERCOM offices work with experts from the Joint Staff and the joint cyber headquarters elements, Cyber Mission Force teams, U.S. Northern Command, National Guard, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), state governments, allies, and the private sector. Our defenders battle in the exercise networks against a world class "opposing force" to make this nearly three-week event as realistic as possible. The idea is to train our forces to operate as they would in an actual cyber crisis – i.e., against live

opposition and alongside the federal, state, allied, and industry partners who would also have authorities and equities in such an event. Over a thousand participants, including representatives from critical infrastructure partners and National Guard teams from 16 states, practice how to collectively protect the nation along with DoD networks. Participants from the Department of Defense practice lending appropriate support to civil authorities, and doing so on a complex exercise network that takes months to fine tune in advance of CYBER GUARD.

This latest iteration of CYBER GUARD was the largest and most realistic yet. Participants got to "maneuver" in cyberspace – seeking to see, block, and ultimately expel from the network adept opponents who had the advantages of knowing what they wanted to take (or break) and who swiftly learned their way around "our" systems. Our defenders thus experienced some of the fast-paced uncertainty of a real cyber campaign, when major decisions have to be made on the fly without the benefit of full insight into the adversary's intentions and capabilities. Players at CYBER GUARD fought through a relentless pace of events and learned that they have to trust each other for their efforts to mesh together and prove effective. To build that trust, moreover, there is no substitute for the sharing of both their information and experiences. Exercises like CYBER GUARD not only teach commanders and units how to see, block, and maneuver in cyberspace, they teach our Soldiers, Sailors, Airmen, and Marines to be teammates, both with one another and with colleagues in other parts of the federal government and private sector who we work beside to make cybersecurity effective.

CYBER GUARD showed us ways to improve our exercising of the total force and also highlighted areas where our attention is needed. This will sound familiar to many Members here assembled. I raise them to provide you with an accurate picture of the challenges in building capability and operating in the dynamic cyberspace domain.

A good analogy here is to the way our military has developed special operations forces. Our special operations forces are as good as any in the world, as we have seen over the last decade and more. Few people realize, however, what it takes for a special operations team in the field to execute a mission. They have an intensive need for critical enablers. This is the case for any maneuver element, and cyber teams are no exception. We have through CYBER GUARD and other exercises and operations a host of mission critical requirements that we are actively acquiring, building, or seeking. The Department and the government are reviewing the scope of authority for our cyber forces, including command and control relationships, manpower guidance, and development authorities to acquire the specialized tools and service we require. We are training cyber warriors and educating cyber professionals, both in the Service schoolhouses and in tailored settings. We are building out the Cyber Mission Force teams, aligning them to missions, customizing their intelligence support, assigning them to commanders, and assessing their readiness (indeed, CYBER GUARD served as a certification event for several teams; among them were teams deployed on real-world missions just weeks later). Across the cyber workforce we are setting the right mix of military and civilian personnel, and working to harmonize the several civilian hiring and career systems that take care of our people who work under parallel but not always equivalent institutional templates.

In particular, we are building a dedicated, persistent training environment, like DoD utilizes in each of the other domains. Let me explain what it is that we are doing. CYBER GUARD took place in Joint Staff facilities in Suffolk, Virginia, giving us the opportunity to practice in a controlled but more or less realistic cyber environment that we did not have to set up ourselves and then tear down after the exercise finished. Nonetheless, this was not the same as exercising in an environment specifically designed to mimic conditions on the Internet and the

real world of cyberspace, where industry partners, for instance, are independently taking steps (such as updating malware signatures and even outing cyber actors) to defend their own systems. While we defend DoD networks, of course, we are helping our federal partners to guard US Government systems as well. We need greater realism to reflect this reality in our training. With the help of the DoD Central Information Officer and others, we are now building out and testing a new exercise environment and working on interagency exercises and testing environments with partners including DHS.

Last but not least is our requirement for vital cyber infrastructure improvements to operate DoD systems safely even under attack. I have explained our need for the Unified Platform and the Joint Information Environment in previous hearings, but I will reiterate how important they are to the defense of DoD's systems and our ability to operate and deliver effects outside the United States. These improvements are the future, for they represent a revolutionary and much-needed change to the Department of Defense Information Networks (DoDIN). In addition, though information sharing alone is not a silver bullet, it is critical that the government and private sector be able to share information that will enhance the situational awareness we need to protect our nation and its interests. I am encouraged by the work that has gone into cybersecurity information sharing legislation in both the House and the Senate. But it is imperative that we finish that work and pass a cybersecurity information sharing bill as soon as possible. Cyber criminals are not waiting to steal intellectual property or financial data, so neither should Congress wait to pass this important legislation. These steps are needed to ensure that cyber remains a strategic asset, not a liability, at this strategic inflection point.

Implementing the DoD Cyber Strategy

Recall Secretary Carter's earlier point: if we cannot defend the infrastructure that undergirds our DoD bases and forces from foreign-based cyber threats, then our nation's military capabilities are weakened and all our instruments of national power diminished. That leaves our leaders with a need for additional options to pursue short of open hostilities, and with fewer capabilities in an actual clash of arms. This raises risk for all by inviting instability and miscalculation, as the Secretary noted.

Our nation has peer competitors in cyberspace, with other nations and groups also striving to deploy advanced cyber capabilities. They do not match our entrepreneurial élan, our manufacturing skill, or our deep investment in the theory and machinery of cyberspace. Yet they have already hinted that they hold the power to cripple our infrastructure and set back our standard of living if they choose. They know, of course, that we can hit back, and that potentially devastating cyberattacks against U.S. interests would ripple across the global economy. But they could well count on deterring us in a regional crisis, making our leaders hesitate and muffle American responses to aggression overseas. Such delays could give them time to continue their encroachments, attain their objectives, and consolidate their gains.

We need to understand the systemic-level implications of what is happening. We are, in effect, being strategically shaped by potential adversaries. They also feel entitled to turn the resources of their states against private business, research labs, academic institutions, and even individual citizens in the West to steal the fruits of our creativity, or negatively impact the enjoyment of human rights and fundamental freedoms, including the freedom of expression.

This context adds the sense of urgency we feel at USCYBERCOM and across the Department of Defense. How do we prevent potential adversaries from shaping us and deterring our defense of America's interests and allies? We know that the DoD Cyber Strategy gained the attention of countries overseas – this enhances deterrence right here. But that is only one step of many. We need to take several more steps as we implement that Strategy.

First, we have to continue the whole-of-government coordination that makes our words and actions far more meaningful to potential adversaries. As Secretary Carter stated in announcing the DoD Cyber Strategy, we need synchronized inter-agency measures to bring all the powers and authorities of the U.S. government to bear on malicious cyber actors. Individual sanctions, indictments and other steps are effective tools, but they might not be sufficient by themselves because potential adversaries believe they have too much to gain from continued cyber-enabled theft of our intellectual property and continued intimidation of their neighbors through cyberspace (among other mechanisms, of course).

Second, we must deepen our partnerships. Organizations across the U.S. Government must create consistent, complementary approaches for operating with private sector and international partners—leveraging the comparative advantages of civilian, homeland security, law enforcement, intelligence community, and military entities. Many departments and agencies share the authorities and responsibilities to guard critical infrastructure in the United States, and we look to DHS' Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT) for information-sharing, incident response and mitigation. We as a nation need to enhance governing policies and legal frameworks to enable a robust defense of the defense industrial base and other sectors of our critical infrastructure. This could include efforts across

the Government to identify and manage risks to our critical infrastructure and key resources in the near term, while transitioning from a reactive to a deterrent posture over the long term.

Finally, we must forge a consensus on when we can and should respond to cyber activity directed against the United States. Such a consensus should clarify the proper role of the military in a whole-of-nation approach to improving our security in the cyberspace domain. The President has stated that we reserve the right to respond with all instruments of national power to cyberattacks against our critical infrastructure. Here is where we particularly need to build trust in the ability of the U.S. Government—on the civilian and military sides—to exercise its powers and capabilities responsibly to defend the nation, consistent with international law and norms. I see my job in this entailing an effort to better explain certain concepts like "offensive cyber operations" and the Cyber Mission Force. I welcome your ideas on this.

Conclusion

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to speak on behalf of USCYBERCOM about the vital topic of cyberspace strategy. Our Command is helping the Department and the federal government mitigate risk while unleashing the promise and opportunity inherent in cyberspace in ways consistent with our values as a nation. As you can tell from the foregoing, I take pride in the accomplishments of our men and women. I know they will give their all in executing our Command's missions and in forging cyber forces that offer our nation's leaders a full suite of options in cyberspace and beyond. With their great efforts and your continued support, I know we can be positioned for success, despite the seriousness of the current situation. There is no single technical or engineering fix alone that is

going to solve these challenges, but instead we will require a great deal of the fortitude, creativity, and determination that we Americans have repeatedly shown we can muster. I look forward to your questions and to advancing this important dialogue.

Admiral Michael S. Rogers
Commander, U.S. Cyber Command
Director, National Security Agency
Chief, Central Security

Admiral Michael Rogers is a native of Chicago and attended Auburn University, graduating in 1981 and receiving his commission via the Naval Reserve Officers Training Corps. Originally a surface warfare officer (SWO), he was selected for re-designation to cryptology (now Information Warfare) in 1986.

He assumed his present duties as commander, U.S. Cyber Command and director, National Security Agency/Chief, Central Security Service in March 2014.

Since becoming a flag officer in 2007, Rogers has also served as the director for Intelligence for both the Joint Chiefs of Staff and U.S. Pacific Command, and most recently as commander, U.S. Fleet Cyber Command/U.S. 10th Fleet.

Duties afloat have included service at the unit level as a SWO aboard USS Caron (DD 970); at the strike group level as the senior cryptologist on the staff of commander, Carrier Group 2/John F. Kennedy Carrier Strike Group; and at the numbered fleet level on the staff of Commander, U.S. 6th Fleet embarked in USS Lasalle (AGF 3) as the fleet information operations (IO) officer and fleet cryptologist. He has also led cryptologic direct support missions aboard U.S. submarines and surface units in the Arabian Gulf and Mediterranean.

Ashore, Rogers commanded Naval Security Group Activity Winter Harbor, Maine (1998-2000); and, has served at Naval Security Group Department; NAVCOMSTA Rota, Spain; Naval Military Personnel Command; Commander in Chief, U.S. Atlantic Fleet; the Bureau of Personnel as the cryptologic junior officer detailer; and, Commander, Naval Security Group Command as aide and executive assistant (EA) to the commander.

Rogers' joint service both afloat and ashore has been extensive and, prior to becoming a flag officer, he served at U.S. Atlantic Command, CJTF 120 Operation Support Democracy (Haiti), Joint Force Maritime Component Commander, Europe, and the Joint Staff. His Joint Staff duties (2003-2007) included leadership of the J3 Computer Network Attack/Defense and IO Operations shops, EA to the J3, EA to two directors of the Joint Staff, special assistant to the Chairman of the Joint Chiefs of Staff, director of the Chairman's Action Group, and a leader of the JCS Joint Strategic Working Group.

Rogers is a distinguished graduate of the National War College and a graduate of highest distinction from the Naval War College. He is also a Massachusetts Institute of Technology Seminar XXI fellow; Harvard Senior Executive in National Security alum; and holds a Master of Science in National Security Strategy.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

SEPTEMBER 30, 2015

RESPONSE TO QUESTION SUBMITTED BY MR. WILSON

Secretary WORK. At this time, we have not taken legal actions or pursued economic sanctions. The Administration remains concerned about Iran's increasing capabilities and malicious activity in cyberspace. The Department works closely with interagency and international partners to enhance cyber defenses. The President is able to use a broad range of tools—including diplomatic engagement, trade policy, and law enforcement mechanisms—to address cybersecurity threats emanating from Iran. [See page 18.]

RESPONSE TO QUESTIONS SUBMITTED BY MR. ROGERS

Secretary WORK and Admiral ROGERS. Only in limited circumstances would the Department have insight into or the contractual right to control a cleared defense contractor's decision to use any particular subcontractor or supplier. Absent suspension or debarment or a statutory restriction on contracting with a prohibited source, our cleared defense contractors would generally not be precluded from using a specific vendor's telecommunications equipment.

However, it is important to note that the Department has several mechanisms in place to help ensure the security of products or services delivered to us and the systems that cleared defense contractors use to store or process sensitive DOD information.

First, the Department requires Program Protection Plans (PPPs) to address the full spectrum of security risks for the critical components contained in our weapons systems, including supply chain vulnerabilities, and to implement mitigations to manage risk to system functionality. In addition to the security requirements applied to deliverable products or services, the Federal Acquisition Regulation (FAR) requires that contractor information systems used to store or process classified information are compliant with the National Industrial Security Program Operating Manual (NISPOM). Additionally, the Defense FAR Supplement (DFARS) requires that contractor unclassified systems that will store or process sensitive Department of Defense (DOD) information must also provide appropriate security for that information.

There are additional statutory authorities available to the Department to limit or exclude vendors in specific circumstances. For example, section 1211 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2006, as amended by section 1243 of the NDAA for FY 2012, and as implemented at DFARS Section 225.77, prohibits the Secretary of Defense from acquiring supplies or services that are on the United States Munitions List through a contract, or subcontract at any tier, from any Communist Chinese military company. In addition, section 806 of the NDAA for FY 2011, as amended by section 806 of the NDAA for FY 2013, has been implemented at DFARS Subpart 239.73, "Requirements for Information Relating to Supply Chain Risk." The clause enables DOD components to exclude a source that fails to meet established qualifications standards or fails to receive an acceptable rating for an evaluation factor regarding supply chain risk for information technology acquisitions, and to withhold consent for a contractor to subcontract with a particular source or to direct a contractor to exclude a particular source. [See page 32.]

RESPONSE TO QUESTION SUBMITTED BY MR. WITTMAN

Secretary WORK. The Department continues to develop and maintain cyberspace capabilities to support full spectrum operations in pursuit of national objectives, and is prepared to defend the nation against cyber threats and provide the President options in crisis or contingency.

To support these strategic goals, the Department is prepared to defend information, information-based processes, and information systems against threats, thus ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation on the Department of Defense Information Network (DODIN) at all security levels.

The Department has established a trained and ready cyber operations workforce with all the technical capabilities necessary to complete missions and support full-spectrum operations. The FY2016 President's budget requests $5.5 billion in FY 2016 (FYDP, $27.4 billion) for the cyberspace operations, an increase of 11 percent. The FY 2016 cyberspace operations budget continues to support: computer network defense, cyber identity and access management, engineering and deployment controls, cryptographic key production and management, cross domain capabilities, workforce development, information assurance and operational resiliency, offensive cyber operations, and cyberspace Science and Technology. [See page 37.]

RESPONSE TO QUESTION SUBMITTED BY MS. DUCKWORTH

Mr. HALVORSEN. The Department has a very mature and active Defense Critical Infrastructure Program and a disciplined Mission Assurance Risk Management process that is used to identify the Department's most critical assets. The process includes working with the DOD Components to identify single points of failure related to DOD OPLANs/CONPLANs, and the Department's other strategic missions. It also includes prioritization of assets for risk management efforts (to include cybersecurity) and resource investment.

The Federal Acquisition Regulation (FAR) language referred to in testimony is actually an August 26, 2015, update to the Defense Federal Acquisition Regulation Supplement (DFARS), DFARS Case 2013–D018, "Network Penetration Reporting and Contracting for Cloud Services. This rule expands upon the existing "Safeguarding Covered Defense Information and Cyber Incident Reporting" clause, which only covered the protection of and reporting of incidents affecting the controlled technical information. The August 2015 interim rule expands the protection and reporting requirements to a broader scope of information (i.e., "covered defense information") which includes controlled technical information as a subset. This interim rule also requires contractors to be compliant with NIST Special Publication 800–171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations". [See page 42.]

RESPONSE TO QUESTION SUBMITTED BY MR. BROOKS

Secretary WORK. The Department of Defense (DOD) Cyber Strategy emphasizes improving cyber collaboration, information sharing, and unity of effort within the Department. The efforts at the U.S. Army Aviation and Missile Research, Development, and Engineering Center (AMRDEC) Cyber Campus, and similar facilities, are consistent with this emphasis. The AMRDEC Cyber Campus at Redstone Arsenal, Alabama, is an organization designed to integrate, in one location, the expertise of multiple DOD and non-DOD organizations that support aviation and missile system cybersecurity. This campus participates in several programs that leverage DOD-wide capabilities in cybersecurity and related areas, such as the Joint Federated Assurance Center and the DOD Software Assurance Community of Practice. [See page 25.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

SEPTEMBER 30, 2015

QUESTIONS SUBMITTED BY MR. FORBES

Mr. FORBES. The Intelligence Community is using commercial cloud computing capabilities to enable important classified missions. If commercial cloud services are able to meet the security standards of the intelligence community, can DOD use commercial cloud services for classified and sensitive missions? Does DOD have particular technical concerns with regard to the capabilities available on the commercial market?

Mr. HALVORSEN. The Intelligence Community's (IC) use of a private, classified instance of the Amazon AWS cloud demonstrates that, when properly configured and separated from public networks and facilities, commercial cloud services can be leveraged to satisfy many of the Department's requirements for classified and sensitive missions. The IC commercial cloud is essentially a private version of Amazon's public cloud that has been built on the IC's premises supporting the Top Secret network. DOD IC components are exploring contract mechanisms to permit DOD applications and data on the IC cloud.

For the Secret environment, it is not the technical concerns that present a significant challenge; rather, it is the time and investment risk associated with acquiring a private cloud that operates solely within that classified environment. The Department is currently in the process of identifying requirements and options for expanding commercial cloud services to support secret networks.

In the unclassified environment, the Department is able to leverage more of the existing commercial infrastructure, which greatly reduces the time and expense necessary to establish a commercial cloud service. The Department continues to work with commercial cloud providers to perform cybersecurity assessments and approve commercial cloud services for use on the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet). As of October 2015, the Department has approved more than 30 commercial cloud services for use within the Department.

Mr. FORBES. Is DOD looking at solutions that can prevent exploits from succeeding via isolation/containerization strategies "at the end point"? What measures are you taking to address the advanced "polymorphic" threats you face?

Mr. HALVORSEN. Yes, DOD is looking at solutions that can prevent exploits from succeeding via isolation/containerization strategies at the end point. The isolation/containment concept is a primary function of DOD's DMZ architecture. By physically and logically separating public, restricted, and private information systems into their own security zones, movement between these zones becomes minimalized and reduces the attack surface.

In regards to polymorphic attacks, DOD has expanded its detection arsenal to include technology designed to identify malicious code behavior through analysis that identifies specific code execution patterns. This addresses the challenge of malicious code variants. Behavioral analytics can be applied at runtime to a specific machine tracing the execution of applications or offline via a sandbox environment.

The ability to detect and react at the endpoints is a key part of DOD's Defense in Depth and Layered Defense strategies. Once a compromise is detected, containment from the rest of the unaffected Information System (IS) and Information Technology (IT) assets requires swift action and the ability to keep the event scope isolated to the smallest area possible. Micro-segmentation, virtual computing, and software-designed networking will enable Cyber Security Providers, Network defenders, and security engineers more options and capabilities to keep the IT and IS at the prerequisite security posture to meet it missions.

QUESTIONS SUBMITTED BY MR. SHUSTER

Mr. SHUSTER. We heard testimony earlier in the week that attribution in cyberspace is much improved, allowing U.S. agencies to identify and target our greatest cyber-based threats. Do you feel you have adequate guidance and the necessary authorities to executive sufficient offensive and defensive cyber-based activities in support of DOD's three cyber missions?

Secretary WORK. Yes, I believe we have adequate guidance and the necessary authorities to execute sufficient offensive and defensive cyber operations in support of

the Department's three cyber missions. Consistent with Presidential guidance and the Department of Defense Cyber Strategy, the Department will streamline its policies and procedures for cyber. This effort will help translate national and departmental guidance and policy for implementation in tactical operations.

Mr. SHUSTER. There are many companies that partner with multiple sectors of the U.S. Government to include DOD, civilian agencies and the Intelligence Community. I recognize that each entity must develop a comprehensive cyber strategy yet I worry that differing strategies among our government entities could create challenges for the companies that work across agencies. What issue areas do you believe are best legislated by Congress for the whole of government and what areas do you recommend we defer to DOD and/or other executive agencies to develop?

Secretary WORK. The Department depends on passing legislation with meaningful measures to address core critical infrastructure vulnerabilities and provisions to facilitate public-private sharing of information. This can be done while ensuring the protection of privacy and civil liberties. The Department appreciates the early steps taken during this session to build consensus on information sharing legislation. The Department also looks forward to progress on other key provisions, such as data breach and cybercriminal provisions, included in the President's legislative proposal submitted earlier this year.

Internally, the Department works continuously with federal interagency partners to develop a whole-of-government approach to ensure all the resources of the federal government are used wisely. The Department also amended its cybersecurity reporting requirements for defense contractors who hold sensitive defense information in their networks. On August 26, 2015, the Department issued an interim rule amending the Defense Federal Acquisition Regulation Supplement to implement section 941 of the Fiscal Year 2013 National Defense Authorization Act, which requires cleared defense contractors to report network penetrations and to allow defense personnel to access those networks to assess the impact of the reported cyber incident.

Mr. SHUSTER. What steps has and can DOD take to prevent malicious attacks similar to the OPM breach from occurring on DOD networks? Given that in many instances cyberattacks on U.S. networks are undertaken by entities linked to foreign military forces, what response do you feel is appropriate to such a malicious cyberattack?

Secretary WORK. Once the Office of Personnel Management (OPM) breach was identified, the Department immediately took a number of steps to mitigate potential impact to the Department's systems. This included scanning systems for indicators of compromise from the breach; mitigating vulnerabilities in other repositories of personally-identifiable information of the Department's personnel; and assessing any network connections between OPM and Department of Defense networks.

The Department's total network attack surface is very large. It is critical to identify, prioritize, and defend the most important networks and data so the Department can carry out its missions effectively.

To stay ahead of cyber threats, Secretary Carter places a high priority on investing in technology and innovation. The Department is enhancing its cyber defense capabilities by building and employing more defendable network architecture in the Joint Information Environment.

Many hackers frequently target the defense industrial base. Network and data protection requires extensive collaboration with the private sector. The collaboration includes sharing defensive information, ensuring that the Department's contractors report attempted and successful cyber intrusions, and encouraging or mandating adherence to cybersecurity standards as appropriate.

In addition to building U.S. cyber defense and cybersecurity capabilities, the United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law. As with attacks in the physical domain, the Administration takes into account the severity of the attack, such as loss of life or property damage, and consider all possible levers, including diplomatic, economic, and military efforts, when contemplating any response.

Mr. SHUSTER. Many of the strategic objectives in the 2015 cyber strategy require significant changes to the services' human capital management programs related to recruitment, retention, training and utilization. Is the human capital enterprise engaging and adapting rapidly enough to achieve the stated objectives?

Admiral ROGERS. [The information referred to is for official use only and retained in the committee files.]

Mr. SHUSTER. Earlier in the week, we heard testimony from industry experts that recommended a "Zero Trust" or "micro-segmented" network to prevent significant data losses. Do you agree with that recommendation and if so, what would be potential barriers to implementing that approach across DOD?

Mr. HALVORSEN. Yes, we agree that a "Zero Trust" concept implemented through "micro-segmentation" has significant advantages for cybersecurity. Implementing these concepts would theoretically allow for 100%, near-real-time inspection of network traffic and, if necessary, isolation and remediation of impacted areas. In a perfect world, micro-segmentation would occur at the lowest possible level; for instance, an individual suite of offices versus an entire organization.

The Department has issued Requests for Information and has reviewed responses received. This information will be integrated into the pilot programs and proof of concept testing as these software-defined networking and network virtualization programs move forward. Lessons learned from the pilots and proofs of concept testing will determine the required skill sets needed to operate and manage micro-segmentation of the DODIN.

The challenges of implementing this concept DOD-wide include three primary factors: First, the technology to implement is still emerging. Although companies like VMWare, Palo Alto, and EMC are bringing products to market, they're not yet complete solutions.

Second, full implementation requires re-engineering and integration at the data center-level rather than at the network-level. DOD is still working to implement a number of virtualization and software-defined networking initiatives across the Department, and the best path forward has not been determined.

Third, the skills and tools to manage the dramatic increase in the number of virtual networks that would occur as a result of implementing micro-segmentation do not currently exist in the Department.

QUESTIONS SUBMITTED BY MS. SPEIER

Ms. SPEIER. During your testimony, you stated that those involved in the spear-phishing attack on the JCS UNCLASSIFED network were punished but were unwilling to discuss specifics in public. Please provide an overview of those involved and their punishments as well as any policies that have been put in place to punish those responsible for breaches.

Secretary WORK and Mr. HALVORSEN. The Department of Defense follows standard investigative procedures to derive an accurate accounting of any situation requiring further investigation. In the case of the Joint Staff spear-phishing attack, the Joint Staff conducted a fact-finding inquiry to determine the facts surrounding the intrusion. In response to the incident, immediate corrective actions were taken addressing those involved; the Director, Joint Chiefs of Staff, led Joint Staff-wide training, and additional comprehensive training was provided for each affected individual prior to reconnecting to the network.

Ms. SPEIER. During your testimony, you stated that those involved in the spear-phishing attack on the JCS UNCLASSIFED network were punished but were unwilling to discuss specifics in public. Please provide an overview of those involved and their punishments as well as any policies that have been put in place to punish those responsible for breaches.

Admiral ROGERS. [The information referred to is for official use only and retained in the committee files.]

QUESTIONS SUBMITTED BY MR. LAMBORN

Mr. LAMBORN. What are you doing to ensure cyber personnel keep critical skills current, such as computer tech and programming languages, which change constantly? More broadly, what are you doing to improve cyber training?

Admiral ROGERS. [The information referred to is for official use only and retained in the committee files.]

QUESTIONS SUBMITTED BY MR. WALZ

Mr. WALZ. Do you believe our current capabilities pertaining to the number of individuals and technical tools is sufficient to deal with the scale of the amount of cyberattacks that the nation faces on a daily basis? If not, how would you rate our risk level due to these lacking resources? High, medium, low?

Secretary WORK. Cyber-attacks are increasing in frequency, scale, sophistication, and consequence. Although the nation will never eliminate all cyber threats, both government and industry, acting together, are taking important steps to reduce cyber risk. The Department of Defense (DOD) is halfway through manning, training, and equipping the Cyber Mission Force, which includes developing capabilities

to defend the nation from a cyber-attack. Additionally, DOD, through efforts such as the Defense Innovation Unit-Experimental, is strengthening interaction with industry to identify breakthrough and emerging technologies to counter the sophisticated cyber threats the U.S. faces. The risk of cyber-attacks against the United States remains high, and the Department must do everything it can to be prepared. This includes continuing to build and equip our Cyber Mission Force and to innovate in partnership with the private sector. Congress can help by expanding DOD's civilian hiring authorities to recruit and retain top talent.

Mr. WALZ. Is there any discussion or efforts taking place in DOD to address and counter the use of social media and the Internet for recruitment purposes by terrorist and extremists groups such as ISIS and Al Qaeda?

Secretary WORK. Yes. The Department of Defense is engaged on multiple fronts to address and counter terrorist and extremist group activities in social media, in close coordination with our interagency and foreign partners as appropriate. More specifically, the Department has a task force focused on supporting interagency and foreign government actions to disrupt foreign fighter movement from their home countries to the Middle East. One of the sources of information used to enable these operations is derived from social media.

Additionally, the Department of Defense plays a supporting role in the Department of State's effort to counter violent extremist ideologies, including providing personnel to augment the Center for Strategic Counterterrorism Communications, which has the mission to coordinate, orient, and inform government-wide strategic communications focused on violent extremists and terrorist organizations. The Department of Defense's efforts alone will not solve the challenge of this contested information environment and adversary propaganda.

The imperative to stay abreast of increasing technological change and our adversaries' rapid adaptation of technology demands that the Department use a thoughtful, strategic approach to achieve success against a mix of adversaries. Simply trying to match our adversaries "tweet" for "tweet" or matching Website for Website would be both fiscally irresponsible and operationally ineffective. Instead, the Department continues to rely on the skills of its personnel to develop thoughtful, well-constructed plans and partnerships with other U.S. Government departments and agencies and with foreign partners, and to leverage a variety of means to disrupt the adversary's narrative, expose its contradictions and falsehoods, and ultimately bring credible, persuasive, and truthful information to audiences who often have significantly differing perceptions and cultural norms than our own. The main challenge today is the size and pace of communications in social media. Our ability to assess the social media environment is challenged due to its broad scope and constantly changing nature.

Mr. WALZ. As DOD continues to develop the Cyber Mission Force, how does DOD plan on measuring its efforts toward progress and readiness on a continuous basis?

Admiral ROGERS. [The information referred to is for official use only and retained in the committee files.]

Mr. WALZ. Is there any discussion or efforts taking place in DOD to address and counter the use of social media and the Internet for recruitment purposes by terrorist and extremists groups such as ISIS and Al Qaeda?

Admiral ROGERS. [The information referred to is classified and retained in the committee files.]

Mr. WALZ. Is there any discussion or efforts taking place in DOD to address and counter the use of social media and the Internet for recruitment purposes by terrorist and extremists groups such as ISIS and Al Qaeda?

Mr. HALVORSEN. Countering the threat posed by terrorist and extremists organizations using the Internet for recruitment purposes is a concern of the Department. I would like to defer to Admiral Michael Rogers, Commander of the U.S. Cyber Command, Director of the National Security Agency on what the Department is doing to combat this threat.

○