[H.A.S.C. No. 112–118]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2013

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED TWELFTH CONGRESS
SECOND SESSION

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES HEARING

ON

BUDGET REQUEST FOR INFORMATION TECHNOLOGY AND CYBER OPERATIONS PROGRAMS

HEARING HELD
MARCH 20, 2012

U.S. GOVERNMENT PRINTING OFFICE
73–790 WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office,
http://bookstore.gpo.gov. For more information, contact the GPO Customer Contact Center,
U.S. Government Printing Office. Phone 202–512–1800, or 866–512–1800 (toll-free). E-mail, gpo@custhelp.com.

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

MAC THORNBERRY, Texas, *Chairman*

JEFF MILLER, Florida
JOHN KLINE, Minnesota
BILL SHUSTER, Pennsylvania
K. MICHAEL CONAWAY, Texas
CHRIS GIBSON, New York
BOBBY SCHILLING, Illinois
ALLEN B. WEST, Florida
TRENT FRANKS, Arizona
DUNCAN HUNTER, California

JAMES R. LANGEVIN, Rhode Island
LORETTA SANCHEZ, California
ROBERT ANDREWS, New Jersey
SUSAN A. DAVIS, California
TIM RYAN, Ohio
C.A. DUTCH RUPPERSBERGER, Maryland
HANK JOHNSON, Georgia
KATHLEEN C. HOCHUL, New York

KEVIN GATES, *Professional Staff Member*
MARK LEWIS, *Professional Staff Member*
JAMES MAZOL, *Staff Assistant*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2012

TUESDAY, MARCH 20, 2012

FISCAL YEAR 2013 NATIONAL DEFENSE AUTHORIZATION BUDGET REQUEST FOR INFORMATION TECHNOLOGY AND CYBER OPERATIONS PROGRAMS

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

FISCAL YEAR 2013 NATIONAL DEFENSE AUTHORIZATION BUDGET REQUEST FOR INFORMATION TECHNOLOGY AND CYBER OPERATIONS PROGRAMS

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Tuesday, March 20, 2012.

The subcommittee met, pursuant to call, at 2:22 p.m., in room 2212, Rayburn House Office Building, Hon. Mac Thornberry (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. MAC THORNBERRY, A REPRESENTATIVE FROM TEXAS, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. THORNBERRY. The hearing will come to order. And again, let me thank our witnesses for your patience as we deal with the schedule which we cannot control. But I appreciate you all being here.

Let me welcome our witnesses and guests to this hearing on the Department of Defense 2013 Budget Request for Information Technology and Cyber Programs.

I appreciate General Alexander and Ms. Takai being back with us. And it is good to see Ms. Creedon here in a somewhat different capacity than we have worked before.

It is striking to me that in the written testimony, General Alexander says in effect that things have gotten worse in cyber over the last year.

We talked last year about the growing threat and our difficulty in catching up. And despite the successes of Cyber Command over the past year, which I do not discount in any way, it still seems to me that the dangers to our Nation in cyberspace are growing faster than our ability to protect the country.

I think it is significant that the Speaker and Majority Leader are planning to bring broad cyber legislation to the House floor next month. And it is also significant that there continues to be bipartisan support for taking action, an effort in which the ranking member, Mr. Langevin, has been instrumental for some years now.

I hope that the Senate will take action on the various proposals that they have before them. But, in a way, we should not kid ourselves. The American people expect the Department of Defense to defend the country in whatever domain it is attacked.

And that means that Cyber Command must be ready, and Congress and the administration must find a way to ensure that it has the legal authorities it needs, and at the same time ensure that the constitutional rights of Americans are protected.

Today, I will be interested in hearing how the administration's 2013 budget request takes us closer to that goal.

Let me yield to the ranking member for any statement he would like to make.

[The prepared statement of Mr. Thornberry can be found in the Appendix on page 33.]

STATEMENT OF HON. JAMES R. LANGEVIN, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Thank you, Mr. Chairman. And thanks to our witnesses for appearing before the subcommittee today.

So much of our national security is dependent upon the reliable and timely flow of information across secure networks. To say that our ability to defend those networks and project power as required into cyberspace is a priority in the area of growth within the Department [of Defense] is, to put it lightly, an understatement.

That is why this hearing could not be more timely.

And let me associate myself with the remarks of the chairman with respect to the threats and the needed attention, extra attention, we need to focus in on this particular area.

Information technology is pervasive across the entire Department of Defense [DOD], operating in the background of the full range of DOD activities from the most mundane administrative tasks to critical wartime functions. It is easy to overlook as a natural part of the environment.

But because it is so pervasive, it must work effectively and efficiently or all of those functions that rely on it grind to a halt. Moreover, if not properly protected from malignant actors, it could also be a significant national security vulnerability and a source of asymmetric advantage to an adversary.

At over $33 billion, IT [information technology] represents a sizable investment in the Department's budget. It is a considerable challenge to stay abreast of all the developing technologies and growing departmental needs under an architecture that provides both strategic vision and appropriate oversight.

Robust, flexible, rapid, and secure are the words not often found together when describing defense programs. But I look forward to learning how the DOD looks to achieve savings in IT expenditures, while still providing the high-quality IT services that the DOD requires.

However, whatever work and resources we devote to providing these IT services will be meaningless if the Department cannot secure them. States, non-state actors, "hacktivists," and criminals are just some of the security challenges that threaten the network.

Although our awareness cyber vulnerability has sharpened over the past few years, I still believe that we don't fully recognize the potential for damage posed by a breached or disrupted network.

It is good to see that in the area of fiscal constraint, therefore the President's budget has preserved our investment in our cyber defense.

Still, there is much to be done. Much of our critical infrastructure remains outside the DOD's protective umbrella, even as DOD relies upon it. The electric grid is but one of many examples.

While I recognize that other Federal agencies and departments may have the responsibility for this aspect of our homeland defense, DOD remains vulnerable as these gaps go un- or under-addressed.

While we have been assured by senior leaders in hearings earlier this year that such external dependencies are being examined, in some cases mitigated, I am interested to know how for the interagency dialogue—how far the interagency dialogue has progressed along these lines on discussions on this point last year.

Fiscal resources are only part of the challenge in the cyber domain. Questions still remain about how and when the United States will conduct the full range of military cyber activities beyond the civil defense of the network.

Some of these questions lie in the development of a robust cyber policy. And some of them may require legislative action.

With that, I look forward to learning more about this and further issues in the discussion today. And I again want to thank our panel for their presence.

Thank you.

And Mr. Chairman, I yield back.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 34.]

Mr. THORNBERRY. Thank the gentleman.

We have before us today, the Honorable Teresa Takai, Chief Information Officer of the Department of Defense; General Keith Alexander, Commander, U.S. Cyber Command; and the Honorable Madelyn Creedon, Assistant Secretary of Defense for Global Strategic Affairs.

Without objection, each of your written statements will be made part of the record. And if you can summarize your testimony in about 5 minutes, then we can go to questions.

We are supposed to have another vote here in roughly an hour or so. And so, hope that will help us move along.

Ms. Takai, please proceed.

STATEMENT OF HON. TERESA TAKAI, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF DEFENSE

Ms. TAKAI. Thank you.

Well, good afternoon, Chairman Thornberry, Ranking Member Langevin, and distinguished members of the subcommittee.

Thank you for this opportunity to testify on the Department's information technology and cybersecurity budget that has been requested for fiscal year 2013.

I would like to describe for you the highlights of that IT and cybersecurity budget request, as well as give you an update on what the Department is doing to modernize IT, that is so important both from the standpoint of a strong cybersecurity defense, but also from the standpoint of effectiveness and efficiency.

The Department's fiscal year 2013 IT budget request of approximately $37 billion includes funding for a broad range of information technology investments that support our mission-critical operations at the tactical edge, on the battlefield, as well as the business support operations.

Included in the overall IT budget is approximately $3.4 billion for cybersecurity efforts designed to ensure our information systems and networks are protected against known cyber vulnerabilities and are resilient to the ever increasing cyber threats the Department and the Nation face.

Among the Department's efforts to improve its effectiveness and efficiency is the consolidation of the Department's IT infrastructure: its networks, computing services, data centers, application and data services, while simultaneously improving the ability to defend that infrastructure against growing cyber threats.

My office is currently leading the implementation of these initiatives as described in our enterprise strategy and roadmap. But it is important that we work closely with the services, Joint Staff, and U.S. Cyber Command to more aggressively modernize our overall information systems.

One of the central pillars of that modernization and effectiveness is to move us to a single joint network architecture. This will allow the Department, and specifically U.S. Cyber Command, to have better visibility into what is happening on our networks and to better defend against cyber attacks.

This will be done in conjunction with our aggressive data center consolidation. We are currently working to eliminate our excess capacity and consolidate into fewer data centers.

We are on track to significantly reduce the number of data centers. And by the end of this year, we will reduce our current inventory of 772 data centers by more than 115.

In addition to these Department-wide efforts, the services and defense agencies have individually taken actions to better position the information enterprise and security posture.

Army has reduced the number of IT applications from 218 to 77 during their BRAC [Base Closure and Realignment] move from Fort Monmouth, New Jersey, to Aberdeen Proving Ground. And that is just one example of the challenges that they have faced and the actions they have taken.

Navy has reduced by 50 percent the number of applications across its 21 functional areas. The Marine Corps has gone from 1,800 applications to only 700 over the past 18 months. And the Air Force has taken aggressive action and reduced its fiscal year 2013 budget request by over $100 million.

As noted above, the $37 billion of the IT budget includes approximately $3.4 billion for our cybersecurity program. This includes funding for cyber network defense, cryptographic systems, communication security, network resiliency, workforce development, development of cybersecurity standards and technologies throughout the Department.

It does include Cyber Command's fiscal year 2013 budget request of $182 million.

I would like to highlight a few areas where I think the Department has made significant progress.

The Department has currently deployed a modular system called Host-Based Security System [HBSS], which enhances our situational awareness of the network and improves our ability to detect, diagnose, and react to cyber intrusions in a more timely manner.

We have currently deployed HBSS on our unclassified and secret networks. Included in our fiscal year 2013 request, are funds to continue the deployment and sustainment of new HBSS capability modules to better harden, and to provide an automated capability to continually monitor the computer's configuration and to improve the human and device identity management capabilities.

We have also taken the lead in assessing the risk of the global supply chain to our critical information and communications technology by instituting the Trusted Defense Systems/Supply Chain Risk Management strategies that were described in a report delivered to Congress in January of 2010.

Another critical success the Department has had is our Defense Industrial Base Cybersecurity and Information Assurance Program. This program offers a holistic approach to cybersecurity to include our classified threat information sharing by the government, with voluntary sharing of incident data by industry in our defense industrial base; sharing mitigation remediation strategies, digital forensic analysis, and cyber intrusion assessments.

Another area that has become increasingly important to the Department, our mission, consumers, and the economy is electromagnetic spectrum. As pressure for access to spectrum continues, I look forward to working with Congress on future spectrum legislation proposals that achieve a balance between expanding our wireless and broadband capabilities for the Nation and the need for access to spectrum to support critical warfighting capabilities in support of our national security.

Thank you very much for your interest in our efforts. I am happy to answer any questions.

[The prepared statement of Ms. Takai can be found in the Appendix on page 36.]

Mr. THORNBERRY. Thank you.

General Alexander.

STATEMENT OF GEN KEITH ALEXANDER, USA, COMMANDER, U.S. CYBER COMMAND, U.S. DEPARTMENT OF DEFENSE

General ALEXANDER. Thank you, Chairman Thornberry, Ranking Member Langevin, and distinguished members of the committee for the opportunity to appear before you today.

I am pleased to be here with Honorable Creedon and Ms. Takai. We have worked closely over the last year on many of these topics that we are presenting for you today.

And I think you will see that we are making great progress. But as you stated, the risks are also increasing.

We have to thank the committee for all the things that you have done to support us in developing Cyber Command and for the funding that we have received. We really appreciate it.

It is a team sport. And one of the things that I would like to put on the table is from our perspective it requires the team of Department of Homeland Security, the Federal Bureau of Investigation, Department of Justice, as well as the DOD team that you have before us here today.

From my perspective, as we look at it, that includes each of the services and the Defense Information Systems Agency; all key partners in helping us do our cyber mission.

We have worked hard to make some progress. And I wanted to talk a little bit about that progress over the next 25—no just kidding—4 minutes.

As you know, the United States relies on access to cyberspace for our national and economic security. Secretary of Defense Panetta and Chairman Dempsey both emphasized that cyber is one of the areas slated for investment in an overall defense budget that will be leaner in the future.

The task of assuring cyberspace access has drawn the attention of our Nation's most senior leaders over the last year. And their decisions have helped to clarify what we can and must do about developments that greatly concern us.

The U.S. Cyber Command, as I stated, is a component of a larger U.S. government-wide effort to make cyberspace safer for all, to keep it a forum for vibrant citizen interaction, and to preserve our freedom to act in cyberspace in defense of our vital interests and those of our allies.

Although Cyber Command is specifically charged with directing the security, operation, and defense of the Department of Defense's information systems, our work and our actions are affected by threats well outside DOD networks, as the ranking member stated; threats the Nation cannot afford to ignore.

What we see both inside and outside the DOD information systems underscores the imperative to act now to defend America in cyberspace.

In my time with you today, I would like to talk a little bit about the strategic context, the last 2.5 minutes, and give you the five key areas that we are doing.

First, cyberspace is becoming more dangerous. The intelligence community's worldwide threat brief to Congress in January raised cyber threats to just behind terrorism and proliferation in its list of the biggest challenges facing the Nation.

Americans have digitized and networked more of their businesses, activities, and their personal lives, and with good reason they worry more about their privacy and the integrity of their data. So has our military.

Dangers are not something new in cyberspace. When I spoke to you last year, I noted the sort of threats that were once discussed in theoretical terms were becoming realities, and actually being deployed in the arsenals of various actors in cyberspace.

We have long seen cyber capabilities directed by governments to disrupt the communications and activities of rival states, and today we are seeing such capabilities employed by regimes against critics outside and inside their own countries, for example, in the Arab Spring.

Cybercrime is changing as well. The more sophisticated cyber criminals are shifting away from botnets towards stealthier, targeted thefts of sensitive data they can sell.

We saw digital certificate issuers in the U.S. and Europe hit last year and a penetration of the internal network that stores RSA's authentication certification led to at least one U.S. defense contractor being victimized by actors wielding counterfeit credentials.

Nation-state actors in cyberspace are riding this tide of criminality. Several nations have turned their resources and power

against us, and foreign businesses and enterprises, even those that manage critical infrastructure in this country and others.

There are five key areas that I would like to walk through that we are working on that I think are important to this committee.

First, building the enterprise and training the force, something that we are working closely on. And, I think, as you think about developing that force and where we need to go in the future, that should be our number one priority.

As Teri mentioned, I think number two is developing a defensible architecture. Three, getting the authorities correct that we need. The teamwork that we have within the government, setting that teamwork right is number four, and perhaps one of the biggest areas that we can do. And finally, a concept for operating in cyberspace, and we have done those things.

In closing, I think we are making progress, as you stated. But we also note that the risks that face our country are growing faster than our progress. And we have to work hard to do that.

Thank you again for inviting me here today.

[The prepared statement of General Alexander can be found in the Appendix on page 51.]

Mr. THORNBERRY. Thank you.

Ms. Creedon.

STATEMENT OF HON. MADELYN CREEDON, ASSISTANT SECRETARY OF DEFENSE FOR GLOBAL STRATEGIC AFFAIRS, U.S. DEPARTMENT OF DEFENSE

Secretary CREEDON. Thank you, Chairman Thornberry and Ranking Member Langevin, for inviting us to discuss the Department's strategies for operating in cyberspace.

I too am pleased to appear here today with Ms. Teri Takai, the DOD Chief Information Officer, and General Keith Alexander, the Commander of U.S. Cyber Command.

We are all here on behalf of the men and women of the Department of Defense who commit themselves every day to ensuring the safety of the United States, both at home and abroad.

Today, I would like to present a brief overview of the Department's efforts in cyberspace. This includes an update on the implementation of the defense strategy for operating in cyberspace, the progress we have made in meeting the goals of the 2010 Quadrennial Defense Review, and the recently released DOD Strategic Guidance for Operating Effectively in Cyberspace.

DOD continues to develop effective strategies for ensuring that the United States is prepared for all cyber contingencies along the entire spectrum from peace to crisis to war.

Importantly, during these times of fiscal constraint, DOD is also taking advantage of the efficiencies that advances in information technology provide. Almost every feature of modern life now requires access to information infrastructure, and DOD is no exception.

We maintain over 15,000 network enclaves and 7 million computing devices in installations around the globe. These networks, upon which DOD relies, represent both opportunities and challenges.

Whereas the threat was once the province of lone-wolf hackers, today, our Nation, our businesses, and even our individual citizens are constantly targeted and exploited by an increasingly sophisticated set of actors.

While it is difficult to get hard data, we believe the cost of these intrusions run into the billions of dollars annually. We know they pose a clear threat to our economy and our security.

We are also increasingly concerned about the threat to our defense industrial base and the Nation's critical infrastructure. We have seen the loss of significant amounts of intellectual property and sensitive defense information that reside on or transit defense industrial base systems.

The loss of intellectual property has the potential to give an adversary leap-ahead technology to achieve parity with some of our most sensitive capabilities.

The Department has been working around the clock, often in close cooperation with the Department of Homeland Security and other agencies, to protect the Nation from these threats.

Last July, DOD released the Defense Strategy for Operating in Cyberspace, the DSOC. This document marked a significant milestone for the Department because it is the first comprehensive strategy to address this new operational domain.

The DSOC built upon the President's National Security Strategy, the International Strategy for Cyberspace, and the Department's Quadrennial Defense Review.

The DSOC guides DOD's military, business, and intelligence activities in cyberspace in support of U.S. national interests.

The Department is currently conducting a thorough review of the existing rules of engagement for cyberspace. We are working closely with the Joint Staff on the implementation of a transitional command and control model for cyberspace operations.

This interim framework will standardize existing organizational structures and command relationships across the Department for the application of the full spectrum of cyberspace capabilities.

Within the U.S. Government, DOD works very closely with our colleagues in the Departments of Homeland Security, Justice, State, Treasury, Commerce, as well as a number of other agencies.

Although DOD maintains robust and unique cyber capabilities to defend our networks and the Nation, we believe strongly in a whole-of-government approach to cybersecurity.

As such, we fully support the Department of Homeland Security's role in coordinating the overall national effort to enhance the cybersecurity of U.S. critical infrastructure.

We also believe that we have to approach cybersecurity from a global perspective. As a result, DOD is pursuing both bilateral and multilateral engagements to enhance our collective security and develop norms of behavior.

We have to respect and remember, however, the delicate balance between the need for security and our cherished rights to privacy and civil liberties.

Make no mistake. DOD is committed to focusing on external actors while ensuring the privacy and civil liberties of our citizens.

Thank you again for the opportunity to appear here today. And I look forward to your questions.

[The prepared statement of Secretary Creedon can be found in the Appendix on page 72.]

Mr. THORNBERRY. Thank you.

I would like to pose a question. I guess, a different question to each of you in this first round.

Ms. Takai, roughly $37 billion is, I think you said, is the Department's request for information technology.

You know, obviously under current law if something doesn't change in January 2013, every program, project of the Department of Defense is going to be cut 8 to 12 percent because of sequestration. So it seems to me particularly in information technology, that that could cause some difficulties.

Can you describe for us, briefly, what that would mean for the programs that you are responsible for?

Ms. TAKAI. Well, there will be a variety of impacts.

First of all, one of the biggest challenges is we have a number of programs underway that will have to take both reductions and potentially—if in fact we are operating under continuing resolution—we will have to take a pause.

So for instance, we have several logistics projects underway in several of the service areas to improve their capability. And those would obviously be affected.

We have several of the IT modernization efforts that are being funded from our operations and maintenance budget that would need to be slowed down.

And then on top of that, of course, those dollars would impact the dollars that we are spending on cybersecurity.

So some of the programs for instance that I mentioned, where we are looking to roll out a process that we call "continuous monitoring" to give us more capability to actually be able to, rather than take in periodic checks, be able to provide the tools to continually look at the network.

So I think what would happen is that many of those programs, we would slow down. And then we would have to prioritize to determine—there may be some selected programs that we would need to prioritize and effectively stop in order to make sure that we were continuing to fund some of the high priority items, for instance, in the cybersecurity area.

Mr. THORNBERRY. Okay, thank you.

Ms. Creedon, last year this subcommittee had several cyber hearings where we tried to understand what the responsibility of the Department of Defense was to defend the private sector in cyberspace.

And really we had a hard time getting an answer.

And I heard in your testimony that we are working through authorities and rules of engagement and a variety of things. But when do you think the administration would be able to go to the private sector and say, "Okay, here is what we will do for you in cyberspace. Here is how we will defend you, beyond that you have got to figure the rest of it out on your own."

Or when can we make clear what the government's—DOD's responsibility is versus other responsibilities?

Secretary CREEDON. There are probably two pieces to this question. But the first is it is the Department of Homeland Security's

role. They are the lead Federal agency to ensuring that there is protection of the ".gov" and also working with the private sector.

So like any other situation where DOD would provide assistance to civil authorities, DOD would provide assistance as needed, as requested, as required, by the Department of Homeland Security [DHS] in the event that there were some sort of an event where DHS required DOD assets, just like in responding to a hurricane. So I mean, it would be very similar to that.

Now the second piece of this is the private sector that is uniquely connected with DOD, the defense industrial base. And so within the defense industrial base, the Department in an effort that is led by the CIO's office, by Ms. Takai, there is a process where we are getting ready to expand the defense industrial base which are our contractors that provide the unique services to DOD.

Now there is a subset of that as well. And that is what has been referred to as the DIB Pilot, the Defense Industrial Base Pilot. And that is yet another subset of these defense industrial base contractors where we are working with them in a unique way to provide additional capabilities to them.

And that program has been in close collaboration with CYBERCOM [U.S. Cyber Command] and also with DHS to provide additional protections to this subset of the defense industrial base, who will then turn around and provide protections to the rest of the industrial base.

And that one, we are in the process of expanding as well.

Mr. THORNBERRY. I hear what you are saying. I am just not completely convinced if we have a big section of the country without electricity that people are not going to look to the Department of Defense and say, "Why aren't you protecting us," or some other sort of scenario.

I think it continues to provide policy challenges more to us and legal challenges more than technical challenges, which is part of the reason I posed the question.

Finally, General Alexander, kind of looking at this from a broad perspective, as you know, and as I mentioned in my opening statement, Congress is working on cyber legislation to try to update some of the laws that had not been updated.

This takes a little beyond maybe Cyber Command, but if you had to name one thing that Congress could do legislatively, that would, in your opinion, be of assistance in defending the country in cyberspace, what one thing or one area do you think would make the most difference?

General ALEXANDER. I think the key thing from my perspective is information sharing.

We need to be able to see an attack on the country, which I think is DOD's domain to defend the country from an attack versus what DHS is doing to help prevent and protect.

So the resilience that they do in the public face, the DOD requirement would—if our Nation is attacked by another nation-state or a non-nation-state actor at a certain point, the Defense Department would step in.

We can only do that if we can see it.

And I think that goes in line with the standing rules of engagement that the policy folks are working along with the criteria that goes with it. So information sharing.

Mr. THORNBERRY.

Thank you.

Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Again, thanks to the panel for your testimony here today.

I guess I would like to press a little further, and the Chairman was raising this point.

How do you feel the unique and powerful capabilities of CYBERCOM, that CYBERCOM possesses, can best be leveraged to protect networks and infrastructure that is outside of ".mil"?

General Alexander. We will start with you.

General ALEXANDER. I was going to pass that to the Honorable Ms. Creedon. But, I think the first part is, I think in extremis the Defense Department would be the natural ones to defend the country.

I believe within the administration, there is general agreement that that is correct. The issue is now what are those circumstances, and how do we do it?

What does the Defense Department do?

Well, the Defense Department is the only one with, not only the defensive capabilities that we have, that Teri Takai talked about, and some of the offensive capabilities that the Nation would need to defend itself.

I think both of those, coupled with the ability for the Defense Department networks to see globally with the intelligence community, are going to be key to defending the Nation.

So that is what needs to be brought to bear. And for us to be successful, we have to partner with industry to share information, to know when some of these events are going on.

I think that is key to it in setting up the framework.

I think the President's paper on cybersecurity that came out in May of 2009, sets the framework for that for the government. So I do think that is the starting point.

And then add to it what the Department did last year, I think, is the next step for showing what we would do.

Mr. LANGEVIN. Very good.

Would you like to comment as well?

Secretary CREEDON. If the Department, I mean, if the country were truly attacked, then the President would have the authority obviously to defend the country however was needed. And DOD would be ready to do whatever it was that the President called upon the Department to do in the event of a real attack.

Now, one of the things, I think, that is important is that in the event of attack, all of the range of options would still be available to the President. So you wouldn't necessarily limit a cyber response. It could be a kinetic response. It could be a diplomatic response. It could be the full range of options available to the President.

But clearly, if there were a real attack, DOD would be ready to do whatever it was called upon to do.

So I think if that was an uncertainty in this realm, I think we believe that the realm of cyberspace is like the realm of any other attack.

Mr. LANGEVIN. General, let me go back to you.

In many ways we are at a tipping point right now with respect to the capabilities of cyber offense, cyber defense, intelligence gathering, if you will, and the degree to which you can talk about this in this setting—and you and I have spoken about this often.

In order to be really effective at being able to defend the country, we have to be as far out from our shores as possible, and far out forward advanced in cyberspace as possible.

When—and I think you may have used this example before, certainly others have—if we saw a missile coming to the United States, the easiest, most effective way to take that down is at its source in the boost phase, same thing with a potential attack on the country.

Will we ever get to the point where we are going to have policy in place that allows Cyber Command to act at the earliest possible stages before an attack is launched, or when it is in its first stages of being formulated or that it might be in fact imminent?

General ALEXANDER. Well, I think the Department is working on the standing rules of engagement that would give us authorities. Now the issue will be what set of authorities will we be given. And what are the conditions under which we could conduct those authorities still have to be determined and ironed out within the administration.

I do think that is at the top of the list of the cyber things that we are working on right now.

I know in USD Policy [Office of the Under Secretary of Defense for Policy] that is one of the key actions that are going on. And we talk about it on a daily basis, pushing some of those forward.

So I am confident that over the next month or two, some of that will actually go through.

Mr. LANGEVIN. Last question before my time runs out. And I just want to return back to the part of my opening statement when I talked about critical infrastructure that resides off ".mil" networks such as the power grid, essential to our military bases, and our ability to conduct full spectrum operations.

What discussions are underway to address the points of vulnerability? And how has the dialogue advanced in the past year?

General ALEXANDER. I take it——

Mr. LANGEVIN. General Alexander.

General ALEXANDER. Yes. I think we are making progress.

As you may know, the Department of Homeland Security and the Defense Department established a joint collaboration element at NSA [National Security Agency] to help bring those two together to actually ensure that we leverage the capabilities of both departments.

In that respect, I think that is going forward well. I think we are making progress.

It hasn't solved the specific questions that you have asked. But it is a starting point for DHS which would be the public face with industry. And they could leverage the technical capabilities of both

NSA and the FBI [Federal Bureau of Investigation] in accomplishing their mission.

I think that is useful. And it keeps us from trying to develop again another NSA or another FBI.

And it is exactly what I think the Nation would want us to do. So we are making progress in that area.

I think, in my opinion, everybody has great intentions in doing it correctly. There is a lot of tough issues here on what is the government's role in this, what is industry's role, and within the government, making sure that we have each of the parts right.

But from my perspective, we are getting that set right. And I am comfortable with the position and the parts that they are giving us to do.

And those are the things that I think the Nation would expect the Defense Department and Cyber Command to do.

Mr. LANGEVIN. Very good, thank you all.

And I yield back, Chairman.

Mr. THORNBERRY. Mr. Conaway.

Mr. CONAWAY. I thank the gentleman.

Ladies and gentlemen, thank you for being here.

Holding a little bit—Ms. Creedon, you mentioned that the rules of engagement are under development.

When do you expect to have those done?

Secretary CREEDON. It is a collaborative process between the Joint Staff and the Office of Policy. And we have been working on these for quite a while.

Mr. CONAWAY. Right.

Secretary CREEDON. And so our hope is, as General Alexander said, is to have these done in a couple of months.

Mr. CONAWAY. Okay. Is there a similar effort at Homeland Security to develop their rules of engagement that you guys coordinate with those guys on?

I don't like the look of surprise on your face.

Secretary CREEDON. I don't know the answer to that question actually.

Mr. CONAWAY. I guess for us this gets back a little bit to what the chairman was talking about, and that is we have got a bifurcated system. We have got Homeland Security with certain responsibilities, and the Department of Defense with others.

And in terms of attack, cyber attacks, it is over before you know what happened. These happen at lightning speed. Even on the threats from the Soviet Union, we had some warning if they were to launch something at us.

And in these circumstances, that warning would be over with, in a cyber-speed. And we wouldn't develop a NORAD [North American Aerospace Defense Command], and put it under a civilian umbrella to say, "alright, you warn them, and then we will tell the Department of Defense what you need to know to what to launch."

And it seems to me that is what we are building here.

And then my question is: is that the best way to defend the country is to have that bifurcation, because I agree with General Alexander. We don't need to replicate, nor do I think we can, because the quality of NSA.

I don't think you replicate it. They have got the best as it is. And so you can't replicate that at Homeland Security, nor would anybody suggest that.

So how do we make this work given two different cabinet agencies?

Secretary CREEDON. The Department of Defense supports DHS in a whole-of-government approach. And this is one of the things that we have been working on through a variety of different mechanisms to make sure that, just like in response to a hurricane, DOD would provide whatever assistance was necessary to DHS to respond.

You know, in the event of any sort of requirement that DHS had from DOD, DOD would respond.

Now, one of the things that we have been doing is working very closely with DHS to make sure that we are tightly integrated through a variety of mechanisms. So General Alexander just mentioned the joint cyber element which is a collaborative effort.

There are other collaborative efforts going on including the extension of the DIB Pilot.

Mr. CONAWAY. Okay.

Secretary CREEDON. We are working with them very closely to make sure that we can provide them everything they need.

Mr. CONAWAY. Okay.

General ALEXANDER. Could I just add to that?

I think if we look at the different roles, the Department of Homeland Security is the public face for what goes on in the United States for helping to set up the standards for resilience, for ensuring the rest of government networks are set.

And it is forensic in nature. When attack has occurred, they bring together a team—or an exploit has occurred, they bring together a team. And we look at that and we figure out what more we could do to set up the defense.

The FBI's role would be one of law enforcement. Is this a criminal act? Was this espionage? And they take the lead in those cases.

Mr. CONAWAY. Yes.

General ALEXANDER. If it is an attack though, now it shifts over to, in my mind, the Defense Department. The issue is can we determine the difference between those.

So——

Mr. CONAWAY. And I don't disagree. I don't disagree with that.

But at that point in time, the damage is done. So that is where—now we are looking back at it, how do we put the hurricane damage back together?

And I get that part. But this——

General ALEXANDER [continuing]. So——

Mr. CONAWAY [continuing]. How do you stop it before it happens?

General ALEXANDER. So we agree that the three centers that we have, between FBI, DHS and DOD, they have to be connected and integrated with people from each of those centers at the other.

So that when an event occurs that is FBI or DHS lead, we all agree that is it.

But when *in extremis,* the worst case is if it is an attack on the Nation. They all see that now it shifts over to a DOD or whoever the President has determined responsibility.

Mr. CONAWAY. Okay——

General ALEXANDER. Because that is where the standing rules of engagement would actually——

Mr. CONAWAY [continuing]. Are those going to be quick enough in cyber to make a difference to stop the attack?

General ALEXANDER. Well, that is what we are pushing for. What I am pushing for is to have those that can actually allow us to prevent——

Mr. CONAWAY. Right——

General ALEXANDER [continuing]. And protect.

Mr. CONAWAY. Okay.

The DIB [Defense Industrial Base Pilot Project], the enhanced project, pilot project, whatever, how do we know that everything that we know that the private sector didn't already know, and that we have over classified or we are protecting data or information or at times modalities that are already known to the private sector?

Where in the team do you look at that and say, you know, this really is a secret that only we know or something that is broader and we don't have to overlap and duplicate things?

General ALEXANDER. That is a great question. I think it can be more easily answered in a classified environment.

I think to hit this though, we do have capabilities that we are able to share the signatures with the companies. And we know, based on their defenses, whether they have that signature or not.

Mr. CONAWAY. Okay.

General ALEXANDER. And so the ability to share that, and we can also see what companies after the fact did not have that because they have been exploited by it.

This is an area where information sharing would be absolutely vital to stopping some of these exploits that are going on right now.

Mr. CONAWAY. All right.

Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank you.

Mr. ANDREWS. Thank you, Mr. Chairman.

I want to focus on something that you have heard from several members of the committee and that is this notion that a huge percentage of our critical assets are in the private sector, and how we deal with that.

I think you have all done a really good job given the way we have collectively defined the problem. But I think we have collectively misdefined the problem.

For years, for a couple of centuries, the way Newton viewed physics was the right way to view it. And the data he collected weren't wrong. They were right given his premises. And then Einstein came along with the theory of relativity and the whole world changed.

And what I am hearing thread through this discussion, I think, is two misperceptions. First is that we centered the jurisdiction to take care of the utility companies, and the commercial sector, and homeland security because this is a threat to the homeland.

I think the question should be: where is the threat from, not what is it to?

And although we have domestic hackers who are criminals, I think that the principal threat that we face would be asymmetric

warfare or state-to-state warfare, propagated by enemies outside the country.

So I would question whether that is the right assumption.

And then the second one is that we have had a lot of discussion here about the rules of engagement once the attack has occurred. I would chime in what Mr. Conaway just said.

The attack has occurred. It is kind of over in a lot of ways. And there is not a whole lot to respond to once a system is corrupted.

I think the premise—the focus ought to be on prevention rather than engagement once the attack has begun. And it strikes me that—well, it strikes me that because these premises are wrong, and this might violate hundreds of years of tradition of Posse Comitatus.

I think if we are worried about a threat coming from outside the United States to attack critical infrastructure, to cripple our economy, our telecommunications systems, our power grid, that the Defense Department ought to be the focal point of the effort, number one, because our technology is more advanced, and because the agency is geared that way.

And number two, I think our focus ought to be hardening our systems to prevent an attack, number one. And then talk about responding to it once it occurs.

What is wrong with that analysis?

Secretary CREEDON. There is a lot in there. Let me unpack it just a tiny bit.

Mr. ANDREWS. All right.

Secretary CREEDON. So first, let me just touch briefly on the international side of it.

So right now, the Department is very much engaged with a number of our allies, particularly our close allies, Canada, U.K. [United Kingdom], Australia, and New Zealand. And we are working with them to enhance our collective security and our collective awareness.

So we are not in this just alone looking outside from here.

So we really are trying to build an international——

Mr. ANDREWS. But if I may, if——

Secretary CREEDON [continuing]. Provide——

Mr. ANDREWS [continuing]. The lead agency to defend us internally is Homeland Security, then it strikes me that an agency that regularly interacts with other governments ought to be the lead here, right?

I mean, Homeland Security doesn't really interact all that much with the intelligence or tech capabilities of Germany or Brazil or whomever, do they?

Secretary CREEDON. Well, they also have through an organization called the Ottawa Five. DHS, as well as other do participate in international forums.

DOD is working with the militaries of our close partners to be prepared and to have the situational awareness.

Now the other thing that helps is information on all the networks. And so the various forms of cyber legislation that are pending, would also allow us additional situational awareness through the information sharing that would be allowed under the authorities that are provided——

Mr. ANDREWS. I am glad that is happening——

Secretary CREEDON. [Inaudible]——

Mr. ANDREWS [continuing]. I am also glad this pilot program is happening.

But I would just suggest to the chairman as the legislation goes forward, one of the things we ought to really be thinking about here, the way I look at it, is that how do we assure that our utility companies, and our banking system, and our power grid people, and then all the others have the hardest systems they can possibly have, and have access to the best available technology on an ongoing basis as they have?

And frankly, my observation would be that we are not there. And it is not because of the efforts of these outstanding people, but it is because the way we define and conceptualize this problem, I don't think is right.

And I would yield back.

Mr. THORNBERRY. I think the gentleman makes some interesting and fair points. Part of my reaction is that is why we need to take this step and a step-by-step, although there is a lot of urgency to be taking some steps.

And so we will have the opportunity to do that, I think, as I mentioned, in about a month on the House floor.

We are going to have to recess. We have got two votes. I apologize for the break.

But we will be back in just a few moments.

And with that, we will stand in recess.

[Recess.]

Mr. THORNBERRY. The hearing will come to order.

Again, thank you all for your patience.

Ms. Takai, I would like to ask you about a couple of areas.

You mentioned in your opening testimony about what I would term essentially consolidation of information databases and so forth.

You know, obviously this is a trend where everybody talks about the cloud, partly for efficiency, partly for convenience. I am sure you have looked at these issues.

One side says that if you store your data in a repository, it is easier to protect. Because you can ensure that the defenses on that data are adequate.

Other people say if you put it all in one place, once you get in you have got everything.

So can you just briefly explain to us your reasoning on protecting the Department's data. And how you think that debate comes out.

Ms. TAKAI. Certainly.

Well, there are two ways I think to look at the way we are approaching moving to a cloud architecture as it relates to our information and our infrastructure.

One of them is that we truly believe that we will be able to, in a more uniform way, protect our information by moving to more standardized platforms and ways of operating from an infrastructure-protection standpoint.

Now, the thing I think that is important, the one point there, is that for us that doesn't necessarily mean one cloud only. With our

size and scope, as we are moving to modernization, as we are moving to consolidation, we will be doing it in stages.

So we will be looking at what services are going to be provided by each one of the military services, and the way they are moving to their own clouds. And then we will be looking at an enterprise cloud to provide services like identity management, enterprise e-mail, some of those things that we need across the Department from an information sharing standpoint.

The second point then though that is important is that as we look at the protection of the cloud, while in fact we are going to be able to better protect as we get more standardized, the other thing is that we are not looking at just the protection at the perimeter of the cloud.

We are looking at actually putting mechanisms in place—and the commercial sector does this in some instances—where in fact, when we know that there will be instances where we may have a breach of the external perimeter of that cloud, and we need to be able to protect at the information level.

And that is why we are focusing very much on identity management so we know who is in the cloud. And we are also linking that to what information that particular individual has access to.

So it is really both of those that really gives us an assurance that as we move to that kind of an architecture, that we will be able to better protect our information.

Mr. THORNBERRY. Okay. Let me change topics completely.

You mentioned spectrum in your opening statement as well. Again from a very broad perspective, my sense is that as we all rely more and more on various devices that connect to the Internet, spectrum becomes a bigger and bigger issue.

Can you just briefly describe for a lay person how you see that moving ahead for the Department of Defense, and how the investments we are making now, where they lead us?

You know, so periodically, you know, we will have a bill. And we will reallocate spectrum in some way or another. But still there is a finite amount to reallocate——

Ms. TAKAI. Right.

Mr. THORNBERRY. And so we are going to have to have a different approach, aren't we?

Ms. TAKAI. Yes, sir. One of the things that we are doing right now is to actually do a spectrum study around our full use of spectrum. And look at what are the issues going forward.

Now some of the things that we are looking at for instance is when do we think there will be viability in spectrum sharing. That is still very much in the early stages. And we are looking at when that might be a viable option.

The second is to your point. Even though and even with the commercial need for spectrum, we also are becoming greater users of spectrum as we move to more unmanned vehicles, as we move to, you know, many of the ISR [intelligence, surveillance, and reconnaissance] capabilities. So we are the users of spectrum as well.

So the other piece is going to be for us to look at how we better use the spectrum that we have. And then thirdly, how we look at some of the less crowded bands of spectrum which in some cases will cost of us more to be able to utilize.

But as we are looking at programs, again to the point you are making, out in 10 to 25 years, how do we make sure that our future acquisition programs are recognizing the commercial demand for spectrum, so that we are pointing those in the direction of where we believe we will have a greater opportunity to have dedicated spectrum going forward.

But again, the challenge is in some of those cases it may mean that there are costs to the programs in order to move there. But when we balance those against the other economic issues that I think we are facing as a nation, that that will be the better way to go.

I think the last thing I would mention is that the challenge around our utilization of spectrum is now very much becoming an international issue. We just finished with this year's World Radio Conference.

And clearly going into the World Radio Conference in 2015, the issue of the utilization of spectrum not only here in North America, but now the growing demand coming out of the developing nations, is also going to make us take a very hard look at the way that we are using spectrum globally.

So those are some of the issues we have coming at us in the future.

Mr. THORNBERRY. I think it is helpful if you and others in the Department can alert us where we may have higher initial costs based on future assumptions about spectrum. That kind of helps explain to us some of the higher initial costs which we are asked to support.

Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman, and thanks to our witnesses for joining us today.

General Alexander, I have got a number of questions that I think are structured in such a way so as to easily elicit a yes or no response. So if I could get your agreement to answer the questions in that way.

And if you want to explain them after, I will certainly give you a chance to explain.

But General Alexander, if Dick Cheney were elected President and wanted to detain and incessantly waterboard every American who sent an e-mail making fun of his well-known hunting mishaps, what I would like to know is does the NSA have the technological capacity to identify those Cheney bashers based upon the content of their e-mails?

Yes or no?

General ALEXANDER. No. Can I explain it?

Mr. JOHNSON. Yes.

General ALEXANDER. The question is where are the e-mails, and where is NSA's coverage?

I assume by your question that those e-mails are in the United States.

Mr. JOHNSON. Correct.

General ALEXANDER. NSA does not have the ability to do that in the United States.

Mr. JOHNSON. What about if the—when you say the e-mails are located—let us make sure we are talking about the same thing.

An American e-mailing another American about Dick Cheney, does the NSA have capacity to find out who those parties are by monitoring—by the content of their e-mail?

General ALEXANDER. No. In the United States, we would have to go through an FBI process, a warrant to get that and serve it to somebody to actually get it——

Mr. JOHNSON. If it were——

General ALEXANDER. [Inaudible]——

Mr. JOHNSON [continuing]. But we do have the capability of doing——

General ALEXANDER. Not in the United States.

Mr. JOHNSON. Not without a warrant.

General ALEXANDER. No, no, we don't have the technical insights in the United States. In other words, you have to have something to intercept or some way of doing that either by going to a service provider with a warrant, or you have to be collecting in that area.

We are not authorized to collect. Nor do we have the equipment in the United States to actually collect that kind of information.

Mr. JOHNSON. I see.

General ALEXANDER. Does that make sense?

Mr. JOHNSON. Thank you. Yes, it does.

General, an article in Wired Magazine reported this month that a whistleblower, formerly employed by the NSA, has stated NSA's signals intercepts include, quote,"eavesdropping on domestic phone calls and inspection of domestic e-mails."

Is that true?

General ALEXANDER. No, not in that context. The question that—or I think what he is trying to raise is: are we gathering all the information on the United States?

No, that is not correct.

Mr. JOHNSON. The author of the Wired Magazine article whose name is James Bashford. He writes that NSA has software that, quote, "searches U.S. sources for targeted addresses, locations, countries, and phone numbers, as well as watchlisted names, key words, and phrases in e-mail. Any communication that arouses suspicion, especially those to or from the million or so people on the agency watchlist, are automatically copied or recorded and then transmitted to the NSA."

Is this true?

General ALEXANDER. No, it is not. Is that from James Bashford?

Mr. JOHNSON. Yes.

Does the NSA routinely intercept American citizens' e-mails?

General ALEXANDER. No.

Mr. JOHNSON. Does the NSA intercept Americans' cell phone conversations?

General ALEXANDER. No.

Mr. JOHNSON. Google searches?

General ALEXANDER. No.

Mr. JOHNSON. Text messages?

General ALEXANDER. No.

Mr. JOHNSON. Amazon.com orders?

General ALEXANDER. No.

Mr. JOHNSON. Bank records?

General ALEXANDER. No.

Mr. JOHNSON. What judicial consent is required for NSA to intercept communications and information involving American citizens?

General ALEXANDER. Within the United States that would be the FBI lead. If it was a foreign actor in the United States, the FBI would still have the lead and could work that with NSA or other intelligence agencies as authorized.

But to conduct that kind of collection in the United States, it would have to go through a court order. And the court would have to authorize it.

We are not authorized to do it nor do we do it.

Mr. JOHNSON. Thank you.

General, the NSA is an agency of the Department of Defense. And you are, in addition to your responsibilities as CYBERCOM commander, you are a director of the National Security Agency.

What limitations does the Posse Comitatus Act place on the NSA's legal authority to intercept domestic communications?

General ALEXANDER. Well, I think the intent of the Posse Comitatus, and the impacts that we have for collecting in the United States are the same. And the fact is we do not do that in the United States without a warrant.

Mr. JOHNSON. Thank you.

And I will yield back.

Mr. THORNBERRY. I thank the gentleman.

Let me—I am not sure. This may be Ms. Takai and General Alexander, but in the 2010 Defense Authorization Act, we passed Section 804, that directed DOD to develop and implement a new acquisition process for IT systems.

And then in the 2011 Defense Authorization Act, we directed DOD to develop a strategy to provide for rapid acquisition of tools, applications, and other capabilities for cyber warfare for the United States Cyber Command, and cyber operations of the military departments.

Can either or both of you all give us an update on where each of those authorities or requirements stand now?

Ms. TAKAI. Yes, perhaps I can start. And General Alexander can add on.

Let me start with the acquisition reform which is the 804.

I think that report was delivered. And we are in the process of implementing those changes.

Those are going—some of those changes that were in the report are going into the DOD 5000 process which I think all of you know is our acquisition process.

In addition, we are implementing many of the recommendations, particularly around what we call "agile development methodologies" that allow us to turn out product much more quickly, in a much more cyclical fashion, if you will, and to take large projects and put them into smaller deliverable chunks.

So there are any number of actions against the 804 that we are in the process of developing and delivering on. And we are actually using those in our project delivery.

As it relates to the rapid acquisition from a cybersecurity perspective, we have all been working with the Acquisition, Technology, and Logistics organization on the response to Congress on that which is known as our 933 Report.

We are actually now all coordinating on what we believe is the final version of that report. In fact, we all saw it over the weekend with the request that we would get our comments back in, because I think that Mr. Kendall knows that that needs to come forward.

It is looking at any number of different areas. It is looking at actually being able to provide General Alexander with several different ways of going at acquisition to make sure that he can turn them more quickly. But also taking recognition that there will be some large project expenditures included in that as well.

So I think you can expect to see that report fairly shortly.

Mr. THORNBERRY. Well, I will just say for myself, if as you work through those issues, if you believe additional authorities are needed, please let us know. Because it makes no sense at all for us to operate at the speed of the industrial age in cyberspace, and then basically that is what we are talking about here.

And so, you know, I will look forward to receiving the 933 Report. But please keep in mind that if you all decide you need additional authorities, we want to know that.

General Alexander it was kind of an interesting conversation with Mr. Andrews a while ago. And part of—it seemed like that conversation was—we know for sure who is launching an attack or exploitation—just in this setting in a brief way, can you summarize the threat in cyberspace as you are seeing it and as Cyber Command has to calibrate its efforts to deal with?

General ALEXANDER. I characterize the threat, Chairman, in three ways.

Largely what we see is exploitation and the theft of intellectual property. That is what is going on in the bulk of the cyber events that we see in the United States.

In May of 2007, we witnessed a distributed denial-of-service attack. Think of that as a disruptive attack against Estonia by unknown folks in the Russian area and around the world, and then subsequently we have seen in Latvia, Lithuania, Georgia, Azerbaijan, Kyrgyzstan.

What we are concerned about is shifting from exploitation to disruptive attacks to destructive attacks.

And what concerns us is that the destructive ones, those attacks that can destroy equipment, are on the horizon. And we have to be prepared for them.

I do think the two things—if I could just state two things more clearly. We talked about the rules of engagement which would be key on this.

We do have rules of engagement in 2004. What we are talking about is updating those to meet this evolving threat. So that is the key that the Department is working on.

The second is we do need DHS in this mix for a couple of reasons.

The Department of Homeland Security, I think, should be the public face for all the reasons. And Mr. Johnson brings out a good one. The American people have to know that what we are doing is the right thing, that we are protecting civil liberties and privacy. And that we are doing this in a transparent manner.

By having DHS working with FBI, NSA, and DOD all together, there is transparency in that. At least the government and everybody will know that we are doing it right.

Two, I think they are the ones that need to set the standards for other government agencies and work with them to ensure those networks are defensible. If we tried to do that, it would sap much of our manpower that you really want us focused on defending the country and going after the adversaries in foreign space.

That is where we should operate. And I think there is synergy there in doing that.

Mr. THORNBERRY. Okay, thank you.

Ms. Creedon, you have, at several times today, mentioned a variety of efforts underway in the administration to update authorities, rules of engagement, a whole variety of things.

It seems to me that there are a host of difficult policy issues involved in cybersecurity, not all of which are DOD-focused. And yet it has been challenging for me at least, to try to get my arms around what the questions are, what those tough issues are.

Are you all—is the DOD policy shop—for lack of a better way to describe it—compiling a list of the tough policy decisions that not just the administration, and not just the government, but the country is going to have to grapple with as more and more of our lives are dependent upon, and even to some degree lived in cyberspace.

Secretary CREEDON. Well, DOD has certainly been working on those things that are within DOD's realm. And among those are some of the issues that we recognize that we share with the other agencies.

And so, I mean, to go back to the legislation again, some of the common elements, but certainly in Lieberman-Collins bill, you know, some of the elements in that bill are the results of the work that the whole interagency, including DOD, have done to identify those things where we really do need some additional input.

So that legislation for instance in terms of coming up with methodologies to protect critical infrastructure protection, so the bill would urge the setting of standards—would direct the setting of standards.

The sharing of information, this again is a very delicate situation where how do we share the right information to make sure that we have visibility into what is going in networks, but are not doing anything to disrupt civil liberties and privacy protection. So, you know, working that sharing issue, working the liabilities issue.

So some of the work that has been done within the interagency that really fleshed out these harder issues where we really do need a system of legislative assistance. Those are in the bills.

The other things we are working internally and those are the things that for the most part DOD believes we can do internally.

Mr. THORNBERRY. Okay. Well——

Secretary CREEDON. With guidance from the President, obviously, because——

Mr. THORNBERRY. Sure.

Secretary CREEDON [continuing]. At the end of the day, it is the President's authority.

Mr. THORNBERRY. Yes. And I appreciate that. I recognize a whole host of proposals are in the administration's cyber legislation draft.

The only thing I would say is that a lot of these issues that probably are DOD exclusively, or DOD-centered, about what is war in cyberspace, how do we defend the country—some of the things that we have talked about already today.

I think that is going to require more than just an internal administration process.

And I would just say that as the policy office and as the lawyers grapple with some of these difficult decisions on what warfare means in cyberspace, that a dialogue between the administration and Congress, and ultimately between the two of us and the country, is really going to be essential.

We will not be able to impose an Obama administration policy on this, or even a government policy on this. It is going to have to be—it is a little bit—I analogize it to TSA [Transportation Security Administration].

Sometimes the government tries something and it is really stupid. And people rebel against it.

And so they rethink. And they find a little smarter way.

And we haven't found a smarter way to do it all yet. But my point is it is part of a give and take on some of these difficult issues.

And I think that is especially true when it comes to Article 1, Section 8, and as it applies to the Congress on declaring war, and how can you do that at the speed of light.

So I know that is kind of long and philosophical. But my point is, it is going to take us working together to work through these issues. And some more dialogue on these tough issues that don't have easy answers, I think would be helpful for the country.

I yield to Mr. Langevin for any questions.

Mr. LANGEVIN. Thank you very much. To the panel again, thank you for your patience today and your testimony and the great work you are doing.

You know, before I begin, the question that Mr. Johnson had asked, I think, you know, this certainly to the degree to which Members have those concerns a question is important to be asked.

It has just been my experience, General, I just wanted to say from a personal perspective, having observed you and interacted with you over the years now, I have always been impressed with the degree which you and the folks at NSA go to the nth degree to try to always "dot the i's" and "cross the t's" and stay within the confines of the law. And it is reassuring that you have that dedication and respect for the other work that you folks are doing, so.

I had a question on the DIB Pilot.

Lessons learned—what lessons have you drawn from the Defense Industrial Base Pilot? And how have you captured the recommendations from Carnegie Mellon's evaluation of the program?

There was some, you know, criticism. Some, you know, didn't think it worked as well as it was intended. And improvements still need to be made.

But can you talk to us about lesson learned.

General ALEXANDER. Absolutely, Congressman.

First, we did the DIB Pilot. As you know, it started in August. And we started the evaluation not too long after.

And so one of the key things that we saw as an issue was how do we share sensitive signatures with industry?

And when we started the pilot, we had not worked our way through sharing all those sensitive signatures with industry in a classified form. And I think the result of that is some of the early results were not much different than what they already get from their own means for getting signatures.

I think once we started sharing those signatures, and it took us a while, so that was our fault. But once we started doing that, and they saw the value of that in specific cases, I think that was a way of turning the corner.

The other thing that became clear as we went into this is industry doesn't always see when somebody is trying to attack or exploit them. And so having a forum that somebody could say, "Hey, somebody is trying to get into your network. You need to know it," is useful for industry as much as it is for government to know when somebody is trying to attack us.

So I think from my perspective, the lessons learned were we have got to be quicker on sharing. I think we have solved that problem. And you can see now we are sharing.

In fact the companies that initially were not as favorable, now have turned that around and have reentered that pilot program. I think that is a huge plus.

And the other one is the information sharing, which is a major part of the legislation. All the legislative packages there which means that we can share with industry, industry can share with us. And we have the ability to tip in queue, from my perspective in real time, optional. But I think that is going to be key to defending ourselves in cyberspace in the future.

Mr. LANGEVIN. Very good.

Anyone else on the panel care to respond to that? Take your question about lessons learned on DIB or did the General cover it?

Okay.

What feedback loop do you have to ensure that what is shared of a classified nature isn't widely known in the industry and thus shouldn't really be classified?

Is that a fair question?

General ALEXANDER. There are two ways of doing that.

If we see information that is widely used, then we should declassify it. In other words, widely available, everybody is seeing it.

If we have sources and methods that are sensitive and classified and not widely used, then I think we would keep that classified.

Think of that as the difference between Enigma and other public forums—if we have an Enigma-like fact in cyberspace, you would want us to protect that.

And the issue is now in cyberspace, but we are going to have to share that with some industry so that they too can be protected from it.

If it is widely known the anti-virus community has it, we should declassify it and get it out. And I think that is the approach that we are trying to take on it.

The issue will be trying to identify those at network speed. And I think we will get better as we exercise in this area. As we work with industry, I think we will get better in doing that.

Mr. LANGEVIN. Fair enough.

Does the DIB in its pilot have an industry ombudsman to help broker the relationship and information sharing exchange between industry and government?

Or is that something that is planned?

General ALEXANDER. Actually, we used the DIB—we actually had an existing relationship that Ms. Takai and her folks ran that we actually used as the forum for starting the sharing relationship with DIB companies.

So we did have that.

And I think that started off pretty good. And it set the framework for how we actually put the DIB process together. It was based on an existing set of relationships that already occurred between the CIO's office and industry.

So that was the starting point. And I think that was a good starting point. And it gave us a basis to go ahead.

Ms. TAKAI. Well, I think it is important to note that out of the total number of DIB companies involved, we have about 200 companies that are in what we call our information sharing effort. And 37 of those are included in the DIB Pilot.

And it is our intention—we have a rule, a Federal rule that is going through now to be able to expand beyond the 200 companies, and be able to roll out to more DIB companies going forward from the standpoint of actually being able to share, both from the standpoint of our threat information, but also in terms of what the companies are experiencing.

And we are seeing a number of areas just based on data collection from those companies that we are getting information on threats that we would not have seen otherwise. And they are getting information from each other as well as from us about what the threats are and what the mitigation could be.

And I think that complements well then the DIB Pilot process which was focused very much around the ISPs [Internet Service Providers] and being able to get some of that protection piece of the information—or taking the information sharing and moving it to the protection piece.

So the two programs really go hand-in-hand. And one builds from the other.

Mr. LANGEVIN. Good.

Secretary CREEDON. If I——

Mr. LANGEVIN. Okay, go ahead.

Secretary CREEDON. If I can just add one piece to this. So as we go forward and we make this pilot permanent, and DHS becomes lead, one of the advantages of having DHS in the lead is that DHS will also then be able to add additional signatures to the process that they see.

And the second piece of this is as we work with the ISPs, the ISPs then can take these capabilities and they can provide those security services to others who utilize their services as well.

So through DHS and through this mechanism of making it permanent, we can actually provide more of an envelope of protection beyond just the defense industrial base folks through the use of the ISPs.

Mr. THORNBERRY. If the gentleman will yield for just a—is there a—one always hears about limits on scalability here. Is there—you said 200 companies going to more. Is there a limit?

Ms. TAKAI. Right now we are going to be limited by the resources because clearly reaching out, working with each of the companies, working through the structured memorandums of understanding that we need to have is going to be our gating factor in terms of number of companies.

General ALEXANDER. If I could, just to help clarify on this. That is under the current thing. If we have information sharing agreements, that greatly simplifies that process.

The technical way essentially allows us to use the power of the Internet. And so this will scale the approach that we are taking in the DIB Pilot in terms of the technical capability to protect all that we need to protect.

Where other solutions that we have put forward do not scale as easily, and are so cost prohibitive that from our perspective going to the DIB Pilot, managed security services, or whatever we call it, is probably the best thing to do for the country and the cheapest, most efficient way.

I think they addressed that problem though is the information sharing thing is key to making that work.

Does that make sense?

Mr. THORNBERRY. Yes, sir. And that is why I wanted to try to delve down into that just a little bit.

And I appreciate the gentleman yielding.

Mr. LANGEVIN. Yes, no, that is a great question.

And obviously I think we all can agree that the most effective defense that we can have, or programs we have to defend our networks is this information sharing aspect. And you have situation awareness, you can see what is coming at you, what to defend against. It is a force multiplier and highly effective.

What about leap-ahead technologies in the R&D realm? Are we any closer—I find that a fascinating statistic that, or fact that the lines of code of the attackers as I understand it has, basing the tax signatures, has stayed relatively constant. And yet the defense—the lines of code in defending against these attacks has grown exponentially.

And how are we doing on the R&D front in terms of, you know, more robust defense?

General ALEXANDER. I have seen, Congressman, those statistics.

What we are seeing is that, you know, the millions of lines of codes that people quote for the defense is for much more elegant defense.

Of course you can come up with a small piece of malicious software that is only 125 or whatever they stated this small thing. But the reality is I think they are in balance.

I think the key thing is the offense has the advantage here. Those exploiting or attacking the system has the advantage.

What we need to do is move to a system then that leverages the power of the network to bring this back.

From our perspective, that is using the capabilities of all the government agencies and industry to bring what we know about that

network and the vulnerabilities that we have to light so that we can defend against them.

I think the other part that Ms. Takai talked about was the going to the IT infrastructure of the future, this thin virtual cloud environment will make it a much more defensible architecture.

I think that is key to the future. Both of those are some of the things that we actually have to go through.

Mr. LANGEVIN. Very good. And my last question, if I could, just going back to the DIB Pilot, in terms of the costs that was some of the concerns that, you know, companies had. You know, who is going to bear the cost for all this?

Where are we on that? Has that been worked out or is it still a work in progress, if you will?

General ALEXANDER. Informally, it looks like the cost per seat per month would be somewhere between 30 cents and $1 or $2. And so the costs have come way down which makes this much more manageable.

So if you had 6,000 seats, you are talking somewhere between, you know, $1,800 and maybe $6,000 a month for that level of service. I think the Internet Service Providers are actually making great progress in this way which would make this something that people would actually say, that is worth doing.

Does that make sense?

Mr. LANGEVIN. Yes. And that is news to me. That is very helpful. I didn't realize that we are moving in the right——

General ALEXANDER. We would like to get it to 30 cents a seat. I think it is going to be somewhere in that range. And I think, you know, depending on what they add in, somewhere in there.

But it is clearly more cost-effective than the way that we were going.

Mr. LANGEVIN. Excellent. Very good, that is good information to have.

With that, I want to thank you all again for your patience today and testimony, the great work you are doing. And look forward to our continued work together. It is a big issue.

And Mr. Chairman, thank you for the time and attention you have given to this issue as well.

Thank you.

Mr. THORNBERRY. Well, thank you. I agree with everything you just said.

I appreciate you all being here, and your patience, and the chance for us to continue to work together on these issues.

With that, the hearing stands adjourned.

[Whereupon, at 4:05 p.m., the subcommittee was adjourned.]

A P P E N D I X

MARCH 20, 2012

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 20, 2012

STATEMENT OF HON. MAC THORNBERRY, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

HEARING ON
FISCAL YEAR 2013 BUDGET REQUEST FOR INFORMATION TECHNOLOGY AND CYBER OPERATIONS PROGRAMS

MARCH 20, 2012

Let me welcome our witnesses and guests to this hearing on the Department of Defense's 2013 budget request for Information technology and cyber programs.

I appreciate General Alexander and Ms. Takai being back with us, and it is good to see Ms. Creedon in a somewhat different capacity.

It is striking to me that in his written testimony, General Alexander says, in effect, that things have gotten worse over the last year. We talked then about the growing threat and our difficulty in playing catch-up. Despite the successes of Cyber Command over the past year, which I do not discount, it still seems to me that the dangers to our nation in cyberspace are growing faster than our ability to protect the country.

It is significant that the Speaker and the Majority Leader are planning to bring broad cyber legislation to the House Floor next month. And it is also significant that there continues to be bipartisan support for taking action, an effort to which the Ranking Member, Mr. Langevin, has been central for some years. I hope that the Senate will take action on the various proposals that have been introduced there.

But we should not kid ourselves. The American people expect the Department of Defense to defend the country in whatever domain it is attacked. That means that Cyber Command must be ready, and Congress and the Administration must find a way to ensure that it has the legal authorities it needs and at the same time ensure that the constitutional rights of Americans are protected.

Today, I will be interested in hearing how the Administration's 2013 budget request takes us closer toward that goal.

Opening Statement of Ranking Member James R. Langevin
House Armed Services Subcommittee on Emerging Threats and Capabilities

Hearing on
Fiscal Year 2013 National Defense Budget Request for Information Technology and Cyber Operations Programs

March 20, 2012

Thank you, Mr. Chairman, and thank you to our witnesses for appearing before the subcommittee today. So much of our national security is dependent upon the reliable and timely flow of information across secure networks. To say that our ability to defend those networks and project power, if required, into cyberspace is a priority and an area of growth within the Department of Defense is, to put it lightly, an understatement. That's why this hearing could not be more timely.

Information technology is pervasive across the entire Department of Defense. Operating in the background of the full range of DoD activities, from the most mundane administrative tasks to critical wartime functions, it is easy to overlook as a natural part of the environment. But because it is so pervasive, it must work effectively and efficiently or all those functions that rely on it grind to a halt. Moreover, if not properly protected from malignant actors, it could be a significant national security vulnerability and a source of asymmetric advantage to an adversary.

At over $33 billion, IT represents a sizeable investment in the Department's budget. It is a considerable challenge to stay abreast of all the developing technologies and growing departmental needs under an architecture that provides both strategic vision and appropriate oversight. Robust, flexible, rapid, and secure are words not often found together when describing defense programs, and I look forward to learning how the DoD looks to achieve savings in IT expenditures while still providing the high quality IT services that the DoD requires.

However, whatever work and resources we devote to providing these IT services will be meaningless if the Department cannot secure them. States, non-state actors, hacktivists and criminals are just some of the security challenges that

threaten the network. Although our awareness of cyber vulnerabilities has sharpened over the last few years, I still believe we don't fully recognize the potential for damage posed by a breached or disrupted network. It is good to see that in this era of fiscal constraint, therefore, the President's Budget has preserved our investment in our cyber defense.

Still, there is much to be done. Much of our critical infrastructure remains outside of DoD's protective umbrella, even as DoD relies upon it—the electric grid is but one of many examples. While I recognize that other federal agencies and departments may have the responsibility for this aspect of our homeland defense, DoD remains vulnerable as these gaps go un- or under-addressed. While we have been assured by senior leaders in hearings earlier this year that such external dependencies are being examined, I am interested to know how far the interagency dialogue has progressed along these lines since our discussion on this point last year.

Fiscal resources are only part of the challenge in the cyber domain. Questions still remain about how and when the United States will conduct the full range of military cyber activities, beyond the simple defense of the network. Some of these questions lie in the development of a robust cyber policy, and some of them may require legislative action. I am looking forward to learning more about that in the discussion today.

Thank you, Mr. Chairman.

STATEMENT BY

TERESA M. TAKAI
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

EMERGING THREATS AND CAPABILITIES

ON

FISCAL YEAR 2013 BUDGET REQUEST FOR INFORMATION TECHNOLOGY AND CYBER OPERATIONS PROGRAMS

March 20, 2012

Introduction

Good afternoon Mr. Chairman and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee on the importance of information technology (IT) to the transformation of the Department of Defense (DoD). I am Teri Takai, and I am the Department's Chief Information Officer (CIO). My office is responsible for leading the Department's information enterprise and ensuring that DoD is as effective and efficient as possible by ensuring that the right information is available to the right people at the right time and the right place. I am responsible for ensuring that DoD information and information technologies can be depended upon in the face of threats by a capable adversary. To do all this in a place as large and complex as the Department clearly requires that DoD information technology be done as a team across all Department organizations. I would like to give you an overview of some important DoD information technologies, technical efforts in cybersecurity, and provide an update on the Department's IT modernization efforts currently underway.

Overview

The Department's FY13 IT budget request of approximately $37 billion includes funding for a broad range of information technology, including: desktop computers, tactical radios, identity management technology, human resource systems, commercial satellite communications, financial management systems, and much more. These investments support mission critical operations that must be delivered in both an office environment and at the tactical edge on the battlefield. These investments provide capabilities that enable the Commander-in-Chief to communicate with and direct the military, support intelligence activities as well as logistics, medical and other business support functions of the Department. The Department's IT environment is even more complex when one considers that these investments operate in over 6,000 locations worldwide, support the unique needs and missions of the three Military Departments and over 40 Defense Agencies and Field Activities within the Department. The Department's IT budget request represents a slight decrease from the FY12 IT budget. This decrease represents savings associated with initial IT effectiveness and efficiency efforts identified by the DoD Components. I anticipate additional savings as the Department implements some of the actions I will describe below. Included in the overall IT budget is approximately $3.4 billion for defensive cybersecurity efforts that are designed to ensure our

information, information systems and networks are protected against known cyber vulnerabilities and are resilient to ever-increasing cyber threats the Department and the nation face. This portion of the IT budget has not decreased and continues to receive the highest-level attention and support of the Department.

DoD's Information Environment

The scale of the Department's networks is illustrative of the complexity of the Department's information infrastructure and IT budget. The networks reach almost every corner of the globe and connect active duty, reserve and national guard as well as civilians and our contractor support base totaling roughly 3.7 million people with active cyber identity credentials issued by the DoD public key infrastructure, or PKI. These credentials are contained on the DoD's common access card, or CAC, and allow each of these people to access the Department's unclassified network and its rich information sharing capabilities. The Department has approximately 25,000 servers that are visible to the Internet, and countless people from DoD's partners access DoD information resources every day and exchange information with DoD personnel.

Information technology is changing rapidly, and DoD is accelerating its efforts to take advantage of the operational, efficiency, and possible cybersecurity improvements of these changes. As an example, we have broad piloting of advanced commercial mobile technologies in every Military Service, and I expect to approve broader deployment of smart phones and tablet computing for unclassified use within the next several months. The Defense Information Systems Agency (DISA) and the National Security Agency (NSA), are working together with industry and have developed security configuration baselines for several of the major smart phone technologies and are working on more. To enable the agile deployment of new and innovative applications to these devices while preserving vital cybersecurity, we are also piloting application storefronts that will be used to manage the configuration of these many devices, and will also be used as a place from which to download new secure applications.

Joint Information Environment

In August 2010, the Secretary directed a number of initiatives to achieve savings in acquisition, sustainment, and manpower costs, while not degrading the Department's ability to execute its missions. Among these is the consolidation of the Department's IT infrastructure, while simultaneously defending that infrastructure against growing cyber threats. Planners from throughout the Department put together a set of initiatives and in the Fall of 2011, the Deputy Secretary signed out the IT Enterprise Strategy and Roadmap (ITESR).

I am currently leading the implementation of this effort, teamed with the Joint Staff along with the Services and many other DoD organizations, to more aggressively modernize the Department's overall information environment. Our primary goals are to make the Department more effective and more secure against cyber threats and vulnerabilities. A secondary, but very important goal is to reduce the cost associated with the Department's overall information technology infrastructure by simplifying, standardizing, centralizing, and automating infrastructure at the enterprise level. We are calling the result of the effort the Joint Information Environment, or JIE. We are using the intelligence community's information technology modernization efforts to inform much of the JIE planning. A team consisting of experts from throughout DoD is currently fleshing out the approach and is developing an implementation plan of action and milestones, and cost estimates.

In addition to benefits for end-users and cyber defenders, the JIE will speed up capability deployment, while making new capabilities easier to defend and more secure. In today's DoD IT environment, a typical IT program develops and integrates the entire IT "stack", which includes the network, the computers, the standard software loads on the computers, and the core machine-to-machine services like messaging, and global load balancing. In addition, the program must integrate cybersecurity across all of this, from operating system configuration, to access controls, to perimeter defenses, to cyber intrusion detection and diagnosis. Today, this effort is replicated for almost every IT program because of the disparate infrastructures and architectures that have evolved in DoD.

In contrast, the JIE will provide program offices an integrated "platform" of network computing, core enterprise services, and security. In many, if not most cases, program managers will be able to build on top of all or a substantial part of this standard platform. With much of the work already done, programs will deliver faster, and will inherit better cybersecurity from the start. Via efforts like DISA's Forge.mil and RACE software development environments, and via integrated test and security evaluation capabilities that match the production platform, we believe we can also help speed up the development, and the quality control and cybersecurity evaluations for programs.

Network Consolidation

One of the central pillars of the JIE is to restructure the Department's networks so as to move DoD to a single, joint network architecture for each security level. For the unclassified network, this is enabled by our new enterprise perimeter defenses. We are currently developing the engineering and architecture details of this JIE element. The goal is to repurpose many of the current, organization-unique perimeter defenses into standard, joint, regional perimeter defenses that will be shared by all DoD organizations within a particular geographic region, and that will all be managed to common operational policies set by Cyber Command. This will provide much more uniform cyber defenses, will allow Cyber Command to be able to "see to the desktops" and will help keep successful intrusions from spreading within the networks, and will improve interoperability and dependability for joint missions.

Data Center Consolidation

The restructuring of the Department's networks will be done in conjunction with data center consolidation. Currently, DoD has an excess of capacity in data centers. The DoD CIO, in coordination with the Services and Defense Agencies, will set standards for the type and design of these data centers. The standards will be essentially identical for the unclassified network (NIPRNET), secret-classified network (SIPRNET), and any cryptographically and/or physically separate mission networks the Department constructs. This consolidation, in conjunction with the move to more enterprise information services, will allow the Department over time to significantly reduce the number of data centers from the more than 770 data centers identified in

our 2011 inventory. By the end of fiscal year 2012 DoD will reduce its inventory of data centers by more than 115.

The objective of this effort is to consolidate DoD existing data centers into three types of standard data centers. Core data centers will be used for information services and applications that must be available broadly across DoD, and for the Department's outward-facing applications and services required for interaction with industry and the public. These will in fact become the initial DoD cloud computing instantiation. We also anticipate establishing regional data centers that will host information services and applications that are better placed closer to end-users in the region. Examples include print servers, thin client servers, and servers that control access to end-user devices. Finally, we also envision the possibility for some forward deployed/deployable data centers. The centers will be flexible and will hold both regional and enterprise services and data, all tailored to the mission situation and to the speed and reliability of the connection to the more fixed portions of the network.

The servers in these computing centers will generally be highly virtualized so as to allow agile insertion of new information services, to provide portability of applications, data, and eventually whole data centers between regions, and to provide maximum efficiency. Like the layout of the enterprise computing centers themselves, the layout of the server virtualization in the enterprise computing centers will be done in accordance with the existing DoD CIO cybersecurity engineering standards and the applicable DoD Security Technical Implementation Guides for server virtualization, for perimeter defenses, and other technologies.

One other significant improvement in this new data center and network structure will be the standardization of the technology for the remote operation of the defenses, the network, the data centers, the servers, and the applications, so as to significantly improve the cybersecurity of the Department's IT control systems. This remote management will be done in accordance with the DoD data center standard, and the applicable cybersecurity standards.

Commodity Purchasing

The Department has achieved cost avoidance estimated at over $3 billion over a 10 year period through our Enterprise Software Initiative (ESI). DoD organizations have achieved significant efficiencies in the purchase of software, hardware and services from the open market. This is achieved as a result of terms and conditions negotiated with vendors whose products appear in the ESI inventory. Our IT Enterprise Strategy and Roadmap emphasizes the increased use of commodity purchasing of hardware, software, and services as a major means of achieving efficiencies. Through the sharing of purchase agreements across organizations within the Department, we are able to minimize the number of purchase vehicles in use, further streamlining our IT acquisition processes.

Enterprise Services & IT Governance

Many commonly used information technology services can be more effectively, securely, and efficiently provided "from the cloud", which means from the core data centers. This centralization can reduce staff, but by centralizing, can ensure the operations and defense staffs are more highly trained and practiced. We are moving more aggressively to enforce the use of common applications and services, like email, web collaboration, search, file storage, video, and voice over IP. The successful web conferencing service called Defense Connect On-line is an early example.

To make this vision of a true enterprise approach to the DoD's information technology work, I am also working with other senior leaders at the Pentagon to ensure that governance of IT investments is viewed at an enterprise level and enables agile delivery of it capabilities and solutions, consistent with authority provided by Congress in the FY10 National Defense Authorization Act under Section 804.

Additionally, we are working to resolve some of the cultural, structural, and other challenges in migrating to enterprise solutions. For example, we believe that the "Cloud First" strategy developed by the Office of Management and Budget (OMB) as part of the 25 Point Implementation Plan to Reform Federal Information Technology Management is a promising approach towards consolidating IT and reducing duplicative IT applications. We have developed

a draft cloud strategy for the Department and will be working hard with the Military Departments, DISA, other Components and industry to implement cloud approaches to better optimize our IT infrastructure and applications in the near future.

The above efforts are all ongoing and being aggressively worked across the Department. In leading these efforts, my office has worked very closely with the Military Department CIOs and had some early successes. Notable examples of this include extensive collaboration with Army, Air Force and DISA to establish an implementation approach for DoD Enterprise Email – an important step toward true enterprise solutions. Similarly, my office is working closely with the Navy and the Under Secretary of Defense for Acquisition, Technology and Logistics as the Navy and Marine Corps transition from Navy Marine Corps Intranet (NMCI) to the Next Generation Enterprise Network, to ensure enterprise-wide and cybersecurity issues are addressed in the release of the Request for Proposal.

The result of these consolidation initiatives will be a DoD Joint Information Environment that provides the warfighter with the required access to information and services needed to accomplish their mission from any location with any device and that are dependable in the face of cyber threats by a capable adversary. This standardized information and network infrastructure will eliminate the organizational barriers to information sharing and eliminate seams which malicious actors can exploit to gain access to vital information or systems. It will also increase the flexibility of defense networks to incorporate or respond to changes in emerging technology by minimizing the disparity within the Department's information architecture.

Cybersecurity

As noted above, the $37 billion of the IT budget includes approximately $3.4 billion for DoD's cybersecurity program. This includes funding for cybersecurity practices, processes, technologies, and operations throughout the Department. Virtually every DoD mission depends on the Department's information infrastructure. These missions often depend on the information and information infrastructures of our mission partners and industry.

The Department exercises leadership of its cyber activities through a close relationship of several Department organizations. In my capacity as the DoD CIO, I am responsible for the information assurance and defense of the Department's information networks and systems. I provide guidance and oversight regarding the day-to-day defense and protection of DoD information networks and systems; IT support to military and joint missions; resilience and reliability of information and communication networks; and overall policy and guidance for the Department's IT investments. I work closely with the Under Secretary of Defense for Policy, and specifically the Assistant Secretary of Defense for Global Strategic Affairs, who is responsible for developing Department's overall cyber strategy and policy. General Alexander, as Commander of Cyber Command is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department's information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allies freedom of action in cyberspace, while denying the same to our adversaries.

We have five primary goals for the department's cybersecurity efforts. The first goal is that customers of the DoD information infrastructure, including the Department's mission partners, can depend on essential information and information infrastructure in the face of cyber warfare by a capable adversary. The DoD's operational environment will always contain cyber threats, and DoD missions have to work, and work well in such an environment.

The second DoD cybersecurity goal is to enable rapid and safe data sharing with any partner a mission requires that is sufficiently rich that mission execution is effective. Almost every DoD mission includes partners from outside the Department; many current solutions to satisfy cybersecurity requirements make it difficult or impossible to timely share mission data.

The third goal is that we still need to be able to protect our sensitive and classified information.

The fourth goal is to protect mission commanders' access to cyberspace. The large, shared infrastructures that DoD uses often let the mission risk assumed by one commander spill into the missions of other commanders. Our network consolidation efforts described above are designed

so that risk can be better managed so that DoD can support multiple missions, with multiple (changing) risk postures, simultaneously.

The final major DoD cybersecurity goal is that technology uptake in DoD is agile. Security requirements and processes are often cited as the reason particular technologies cannot be fielded, or are slow to be fielded. We are focused both on changing processes to better enable agile technology uptake, and on deploying technologies that can lower the risk in our use of new and/or poorly understood technologies.

Given the complexity of the cybersecurity problem, and of DoD's information technology environment, we have a wide range of technical and operational efforts aimed at achieving these goals. To achieve the dependability and secrecy goals, we have efforts to remove vulnerability, to shield latent vulnerabilities by laying defenses, and to ensure we know where vulnerabilities still exist. In spite of our best efforts to harden our systems, an adversary may still succeed, so we also have a variety of efforts to detect, diagnose, and react to successful or partially successful cyber intrusions.

An example of one of our Department-wide hardening projects is our effort to configure every DoD computer securely, keep each configured securely as new vulnerabilities are discovered, and ensure the right people know how the computer is configured. To help make this possible, this year we acquired a commercial tool we call the Assured Compliance Assessment Solution (ACAS) that all DoD Components will use to scan for configuration vulnerabilities, then report and fix these. The tool is currently undergoing final testing and will be released for deployment by this summer. Components will be deploying and operationalizating this capability over the next 18 months.

Another example, that spans the hardening, situational awareness, and cyber intrusion detection, diagnosis, and reaction areas is a modular system used throughout the department called the Host-Based Security System, or HBSS. The Department has currently deployed HBSS onto every DoD computer that connects to the unclassified or secret networks. This tool can sense and report vulnerability, shield against certain kinds of cyber intrusions, and detect and react to

others. Since it is modular, HBSS allows the DoD to deploy new hardening, situational awareness, and cyber intrusion detection, diagnosis, and reaction capabilities relatively easily by using the already-deployed HBSS software and management system. Among the cybersecurity funding requested in FY13 are funds to continue deployment and sustainment of new HBSS capability modules to better harden, to provide an automated capability to continually monitor the computer's configuration, and to improve human and device identity management capabilities across the Department.

Finally, starting this year and deploying for the next several, we have an effort to collect information from both ACAS and HBSS about the state of every DoD computer's configuration, and to use this to automatically generate mission risk scores that can be used by commanders at every level. Commanders can use this both to fix the vulnerability, and to better understand where particular missions have vulnerability. The effort is called continuous monitoring, and is being piloted in several places in DoD now. We expect to begin rolling the capability out operationally later this year.

Another key part of hardening is our effort to drive anonymity out of the networks. I discussed the DoD's deployment of Public Key Infrastructure (PKI) identity credentials on the unclassified networks earlier. This calendar year we will complete the issuance of PKI credentials to every one of the 500,000 people who use the Department's Secret network, and by March of next year we will require the use of these credentials. This will not only help us improve accountability for information access, but as we work with the rest of the Government to deploy such credentials across the Federal government will make interagency sharing safer and easier.

I would also like to point out progress and priorities in several other cybersecurity initiatives. Rapid uptake of advanced commercial technology remains a key DoD advantage. While globally sourced technology provides innumerable benefits to the Department, it also provides foreign sources with increased opportunity to compromise the supply chain by inserting malware into technology in order to access or alter data, and intercept or deny communications. In response to these risks, DoD is in the process of institutionalizing the Trusted Defense Systems / Supply Chain Risk Management (SCRM) strategies described in the Report on Trusted Defense

Systems delivered to the Congress in January 2010. DoD is also partnering with other Departments and agencies to explore approaches to managing supply chain risk within critical infrastructures.

Another critical success the Department has had is the DoD's Defense Industrial Base (DIB) Cybersecurity and Information Assurance (CS/IA) Program that DoD CIO oversees. This program offers a model standard for government-industry voluntary partnerships on cybersecurity. The program offers a holistic approach to cybersecurity, to include classified threat information sharing by the government, with voluntary sharing of incident data by industry; sharing of mitigation and remediation strategies, digital forensic analysis, and cyber intrusion damage assessments. While threats cannot be eliminated, this program enhances each DIB participant's capabilities to mitigate the risk, thereby further safeguarding DoD information that resides on, or transits, DIB unclassified networks. The Department's DIB CS/IA Program was the baseline program underlying the DIB Cyber Pilot which established an information sharing construct with Commercial Service Providers to provide managed security services enhanced by government threat information to Defense Industrial Base companies. In partnership with Homeland Security, we are working together on plans make it a permanent program for the Defense Industrial Base.

My office is doing many other things to stay on top of the cyber threat, but we must stay vigilant. The Department's cryptographic equipment must be modernized. We are analyzing the full extent of the cryptographic modernization requirement this year, and will use the data to build a 20 year modernization program with the military services. We have already completed analyses of the COMSEC modernization needs for nuclear command and control and are pursuing modernization. We have made substantial progress in planning replacement of legacy cryptographic equipment in tactical radios, and we are beginning the analysis of the other deployed cryptosystems in DoD.

IT Investment Planning

Additional changes to Department processes are necessary to ensure we can keep abreast of technological advances and defend the network against emerging cybersecurity threats.

In particular, changes to the Department's three core processes (requirements, budgeting, and acquisition) are required to address the systemic conditions resulting in DoD's stove-piped IT infrastructure. My office is working closely with the office of the Deputy Chief Management Officer on efforts to develop a flexible, agile acquisition process that also addresses the DoD's requirements and budgeting processes to institutionalize the agility and flexibility necessary in this rapidly evolving domain.

Workforce Development

A very important element of the Department's out-year cyber defense strategy is ensuring that the right workforce is in place. This means the workforce is properly sized, properly trained and has career paths that encourage growth and development of cyber defense and related skills (system management, cyber mission management, cyber operations, etc.). The Department's IT modernization effort includes a strong cyber defense workforce component that is an integral part of the Department's larger information technology and cyber workforce.

Spectrum

Another area for which I am responsible, which has become increasingly important to the Department's missions, consumers, and the economy of the nation is electromagnetic spectrum. The use of the electromagnetic spectrum continues to be a critical enabler of our warfighting capabilities and cyber operations. Defense leadership is cognizant and sensitive to the unprecedented spectrum demands resulting from the Department's increasing reliance on spectrum-dependant technologies and the rapid modernization of commercial mobile devices. Fully recognizing the linkages between national security and economic prosperity, the Department is investing in technologies and capabilities aimed at more efficient uses and management of spectrum, and for increased interoperability with our Coalition partners and with Federal, State, and Commercial entities. I look forward to working with Congress on future spectrum legislative proposals that achieve a balance between expanding wireless and broadband capabilities for the nation and the need for access to support warfighting capabilities in support of our national security.

Conclusion

Maintaining information dominance for the warfighter is critical to our national security. The efforts I've outlined today will ensure that the Department's information capabilities provide better mission effectiveness and security, and are delivered in a manner that makes the most efficient use of financial resources. I ask that you strongly support, authorize, and fund the Department's key cybersecurity and Information Technology modernization programs. I want to thank you for your interest in our efforts and I am happy to answer any questions you may have.

Teresa M. Takai

Chief Information Officer

Teri Takai is the Department of Defense Chief Information Officer (DoD CIO). She serves as 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. She 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.

Ms. Takai previously served as Chief Information Officer for the State of California. As a member of the Governor's cabinet, she advised the governor on the strategic management and direction of information technology resources as the state worked to modernize and transform the way California does business with its citizens.

As California's CIO, Ms. Takai led more than 130 CIOs and 10,000 IT employees spread across the state's different agencies, departments, boards, commissions and offices. During her tenure as State CIO, Teri pursued an agenda that supports viewing California's IT operations from an enterprise perspective, including: Forming a Project Management and Policy Office, release of the California Information Technology Strategic Plan, passage of the Governor's IT Reorganization Proposal, establishing a Capital Planning Process and directing agency consolidation activities.

Prior to her appointment in California, Ms. Takai served as Director of the Michigan Department of Information Technology (MDIT) since 2003, where she also served as the state's Chief Information Officer. In this position, she restructured and consolidated Michigan's resources by merging the state's information technology into one centralized department to service 19 agencies. Additionally, during her tenure at the MDIT, Ms. Takai led the state to being ranked number one four years in a row in digital government by the Center for Digital Government. Additionally, in 2005, Ms. Takai was named "Public Official of the Year" by Governing magazine. She is also Past-President of the National Association of State Chief Information Officers and currently serves on the Harvard Policy Group on Network-Enabled Services and Government.

Before serving in state government, Ms. Takai worked for the Ford Motor Company for 30 years, where she led the development of the company's information technology strategic plan. She also held positions in technology at EDS and Federal-Mogul Corporation. Ms. Takai earned a Master of Arts degree in management and a Bachelor of Arts degree in mathematics from the University of Michigan.

STATEMENT OF

GENERAL KEITH B. ALEXANDER

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

20 MARCH 2012

Thank you, Chairman Thornberry, and Ranking Member Langevin, for inviting me to talk to you about Cyber Command. I am here representing Cyber Command, with an authorized staff of 937, and operational Service cyber components totaling over 12,000 men and women, whose great work helps to keep our nation more secure. Their ranks include uniformed members of all the military Services and the Coast Guard, as well as civilians and officials from several federal agencies partnered with us in our missions. There is no finer group of Americans anywhere, and the work they do is vital to our security now and in the future. I am proud and humbled to be associated with them.

The Fiscal Year 2013 President's Budget for Cyber Command provides $182 million dollars and 937 personnel to perform our global mission. As demand to develop and integrate capabilities into cyber planning and operations continues to grow, we continue to work with the Department to shape our resource requirements and workforce to provide the necessary level of effort against growing mission sets and threats. I last spoke to the committee in open session just about a year ago. Since then, Cyber Command has made substantial progress in building capabilities to perform its missions. I hasten to add, however, that our nation's need for mission success has also grown, both in its scope and in its urgency. Secretary of Defense Panetta recently told Members that "our adversaries are going to come at us using 21st Century technology," including cyber threats. Chairman Dempsey amplified that statement, noting that we are "very concerned about cyber." Both emphasized that cyber is one of the areas slated for investment in an overall Defense budget that will be leaner in the future. The United States relies on access to cyberspace for its national and economic security. The task of assuring cyberspace access continued to draw the attention of our nation's most senior leaders over the last year, and their decisions have helped to clarify what we can and must do about developments that greatly concern us.

Cyber Command is, of course, a component of a larger, U.S. Government-wide effort to make cyberspace safer for all, to keep it a forum for vibrant citizen interaction, and to preserve our freedom to act in cyberspace in defense of our vital interests and those of our allies. Although Cyber Command is specifically charged (among other missions) with directing the security, operation, and defense of the Department of Defense's (DoD) information systems, our work and our actions are affected by threats well outside DoD networks; threats the nation cannot afford to ignore. What we see, both inside and outside DoD information systems, underscores the imperative to act now to defend America in cyberspace. In my time with you today, I want to talk about that larger, strategic context, to note some recent changes in the ways that we express our cyber posture in public, and to explain what these developments mean specifically for the progress of Cyber Command and the larger cyber enterprise.

Strategic Context

In framing my comments on our progress at Cyber Command, I have to begin by noting a worrisome fact: cyberspace is becoming more dangerous. The Intelligence Community's world-wide threat brief to Congress in January raised cyber threats to just behind terrorism and proliferation in its list of the biggest challenges facing our nation. You know this if you are a national leader or a legislator, a military commander, a corporate executive or chief information officer, or just an ordinary citizen shopping or spending leisure time on-line. Out of necessity, more and more of the time and resources that every American spends on-line are being consumed by tasks to secure data, encrypt drives, create (and remember) passwords and keys, and repeatedly check for vulnerabilities, updates, and patches. Americans have digitized and networked more of their businesses, activities, and their personal lives, and with good reason they worry more about their privacy and the integrity of their data. So has our military. Those Americans who are among the growing

number of victims of cybercrime or cyber espionage, moreover, are also spending their time trying to figure out what they have lost and how they were exploited.

Dangers are not something new in cyberspace, of course. Observers theorized about hypothetical cyber attacks on data and information systems twenty years ago. When I spoke to you last year, however, I noted the sort of threats that were once discussed in theoretical terms were becoming realities and actually being deployed in the arsenals of various actors in cyberspace. I specifically use the broader term "actors" instead of "states." In 2010 we saw cyber capabilities in use that could damage or disrupt digitally controlled systems and networked devices, and in some cases we are not sure whether these capabilities are under the control of a foreign government. Furthermore, we believe it is only a matter of time before someone employs capabilities that could cause significant disruption to civilian or government networks and to our critical infrastructure here in the United States.

We have long seen cyber capabilities directed by governments to disrupt the communications and activities of rival states, and today we are also seeing such capabilities employed by regimes against critics inside their own countries. Events during the Arab Spring last year offer a wealth of examples. As you know, popular protests against authoritarian rule raised hopes across the Maghreb and beyond—hopes that were organized, informed, and expressed in no small part by expanded capacity for communications and the new social media applications that use it. The response of the former regimes in Egypt, Libya, and Tunisia—and some current regimes as well—was to try to filter, disrupt, or even shutter these channels for news and communications, whether to stifle ongoing protests by their own citizens or to keep their peoples from hearing that discontent in other lands had toppled autocratic regimes. Some regimes, moreover, even reach out via cyberspace to harass political opponents beyond their borders.

Cyber crime is changing as well. In part this is due to heightened security and wariness among governments, businesses, internet service providers (ISPs), and average users. Law enforcement and ISPs, for example, have gotten better at identifying "botnets," banks of computers slaved together for criminal purposes, and have become more skilled at neutralizing them. But now the more sophisticated cyber criminals are shifting away from botnets and such "visible" means of making money and toward stealthier, targeted thefts of sensitive data they can sell. Some cyber actors are paying particular attention to the companies that make network security products. We saw digital certificate issuers in the U.S. and Europe hit last year, and a penetration of the internal network that stored the RSA's authentication certification led to at least one U.S. defense contractor being victimized by actors wielding counterfeit credentials. Incidents like these affect DoD networks directly, targeting them with similar malware, often spread by clever "phishing" e-mails that hit an information security system at its weakest point—the user. Nation-state actors in cyberspace are riding this tide of criminality. Some of these actors can and may turn their resources and power against U.S. and foreign businesses and enterprises, even those that manage critical infrastructure in this country and others. State-sponsored industrial espionage and theft of intellectual capital now occurs with stunning rapacity and brazenness, and some of that activity links back to foreign intelligence services. Companies and government agencies around the world are thus being looted of their intellectual property by national intelligence actors, and those victims understandably turn for help to their governments.

The expanding popularity of social media and wireless consumer electronics is driving cyber crime as well. More and more malware is written for wireless devices, particularly smartphones, and soon, we anticipate, for tablets as well. These criminal gangs are trying to exploit social media users and wireless networked systems, but can also exploit our Soldiers, Sailors, Airmen, and Marines in their purely social activities. Real and potential

adversaries can and do learn a great deal about our personnel, procedures, and deployments by monitoring the use that our people make of popular social media. As our military goes wireless these threats to our weapons systems, communications, databases, and personnel demand attention.

Finally, I need to mention a recent development of concern to us at Cyber Command and across our government and allies. Last year we saw new prominence for cyber activist groups, like Anonymous and Lulz Security that were encouraging hackers to work in unison to harass selected organizations and individuals. The effects that they intentionally and indirectly cause are chaotic and perhaps exaggerated in the popular media, but the work of preventing those effects from disrupting DoD information systems does draw attention and resources. We are also concerned that cyber actors with extreme and violent agendas, such as al Qaeda affiliates or supporters, could draw upon the experiences and ideas of more sophisticated hactivists and potentially use this knowledge for more disruptive or destructive purposes, though it remains unclear what the likelihood of such an event is.

Our National Cyber Posture

The American people have rightly come to expect broad and economical access to cyberspace. They have saved their personal information, business files, research projects, intellectual capital, and recreational pursuits in digital formats and stored in networked computing devices. Moreover, they have built social and professional webs of contacts in cyberspace—the all-important "who you know"—and have thus come to rely on the accessibility of these networks. Our military and our government have done likewise. This increased inter-connectedness of our information systems, combined with the growing sophistication of cyber criminals and foreign intelligence actors, has increased our risk. Our inter-connectedness is now a national security issue. Ensuring and securing our computing systems has focused the energies of

America's leadership at both ends of Pennsylvania Avenue and in the Cabinet departments. Recent decisions have helped to clarify our posture for defending net users and the nation in cyberspace, and have sent strong signals to anyone who might impair our interests in this domain.

The President confirmed our inherent right to protect ourselves against attacks in this domain, as in the traditional domains, last spring in his International Strategy for Cyberspace, saying "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country." We reserve the right to use all necessary means — diplomatic, informational, military, and economic — as appropriate and consistent with applicable international law. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible. As in the other domains, of course, the United States will seek to exhaust all options before employing military force, and will seek international support whenever possible. Cyber Command exists to ensure that the President can rely on the information systems of the Department of Defense and has military options available for his consideration when and if he needs to defend the nation in cyberspace.

President Obama and Secretary of Defense Panetta have recently reviewed our nation's strategic interests and issued guidance on our defense priorities. In Sustaining U.S. Global Leadership: Priorities for 21st Century Defense, the Secretary focused on protecting access throughout the domain. For Cyber Command, this means we must pay attention to the ways in which nations and non-state actors are developing asymmetric capabilities to conduct cyber espionage—and potentially cyber attacks as well—against the United States as well as our allies and partners. In this context, our cyber capabilities represent key components of deterrence. Since modern forces cannot operate

without reliable networks, we will invest in advanced capabilities to defend them even in contested environments.

The Department of Defense recently added detail to that position. In accordance with the President's International Strategy, the Department further explained our deterrent posture to Congress in its "Cyberspace Policy Report" last November. DoD's components, particularly Cyber Command, seek to maintain the President's freedom of action and work to dissuade others from attacking or planning to attack the United States in cyberspace. We will maintain the capability to conduct cyber operations to defend the United States, its allies, and its interests, consistent with the Law of Armed Conflict. Our indications and warning and forensic intelligence capabilities necessary to identify our enemies and attackers in cyberspace, moreover, are improving rapidly. As the Department's report to Congress noted, the co-location of Cyber Command with the National Security Agency provides our Command with "unique strengths and capabilities" for cyberspace operations planning and execution. I can assure you that, in appropriate circumstances and on order from the National Command Authority, we can back up the Department's assertion that any actor contemplating a crippling cyber attack against the United States would be taking a grave risk.

Cyber Command works with a range of partner agencies in the U.S. government and among our allies, along with parallel efforts in private industry, to strengthen the overall defense of our citizens, the nation, and allies in cyberspace. The Departments of Defense and Homeland Security collaborate on various initiatives, including the Defense Industrial Base (DIB) Cyber Pilot, a test program to establish a construct for Commercial Service Providers to provide managed security services enhanced by government threat information to Defense Industrial Base companies; and the Enduring Security Framework, an executive and working-level forum with key partners in the commercial technology marketplace.

Finally, I want to assure you that all of our work is performed with our responsibility to safeguard the privacy and civil liberties of U.S. persons very much in our minds. We take very seriously, in all of our operations, our duty to ensure that defending the Department of Defense's information systems and the nation's freedom to access cyberspace does not infringe on Americans' civil liberties, those rights guaranteed by the Constitution that I and every member of my Command swore an oath to uphold.

Building the Enterprise

Cyberspace has a scope and complexity that requires inter-agency, inter-service, and international cooperation. Within the Department of Defense, cyberspace issues are handled by our Command and a diverse set of other agencies and organizations, many of which have their own initiatives with government, allied, and industry partners. It is important to keep this context in mind as I review the efforts, accomplishments, and challenges of Cyber Command.

When I spoke to you a year ago, our Command had just become operational. Just a year later, we have a record of success. We are in action every day making the Department's networks more secure and its operations more effective. We are actively directing the operation of those networks and making commanders accountable for their security. Let me tell you about some of our recent successes:

- This time last year, sophisticated cyber intruders compromised the security of the algorithm employed in tokens distributed by the RSA Corporation. This was very serious news, since a large number of enterprises, including some in the Department of Defense, rely on

two-factor authentication using RSA tokens. Indeed, the systems of some non-DoD users were breached not long after the compromise by intruders exploiting the stolen certificates. Cyber Command had immediately recognized the danger to DoD information systems, warned those DoD networks at risk, and took swift mitigation efforts. We at Cyber Command directed and oversaw the replacement of all RSA tokens throughout DoD. Partly as a result of our actions, we have not seen any intrusions of DoD networks related to the RSA compromise.

- Just a few months ago, we saw an example of how Cyber Command has improved DoD's cybersecurity. In late 2010, cyber actors took advantage of a vulnerability in Adobe software that allowed them to install malicious software on computers whose users clicked on an apparently harmless link, a ruse called spearphishing. In that case, as Cyber Command was just beginning, several DoD networks/systems were breached and our experts could only react to stop files from being stolen and new breaches from being opened. A year later, by contrast, our defensive posture and cyber command and control processes had matured to the point where we were prepared not just to react but to counter such tactics. When another Adobe vulnerability was discovered in late 2011, Cyber Command quickly took action to ensure that no one would be able to use it against us. Sure enough, malicious cyber actors seized upon the vulnerability and used it to mount a spearphishing campaign targeting DoD networks. This time we were waiting and were able to block this campaign from exploiting our systems and acquiring any DoD files.

- The year 2011 might well be remembered as the Year of the Hacker. Various on-line groups garnered headlines for their efforts to publicize

causes of concern to them by breaching the security of government and private networks. The on-line collective calling itself Anonymous, to mention just one of these groups, announced several attempted attacks against Department of Defense information systems. Cyber Command was able to direct and integrate pro-active defensive cyber operations to successfully counter these threats. Over the past year, there have also been related, well-publicized examples of major exploitations or attacks against Defense contractors and other holders of intellectual property vital to our national security. The Cyber Command-led defense of the Department's information systems, however, prevented any of these threat actors from having a similar effect against DoD networks. Finally, the investigation of the WikiLeaks breach continued, and its progress was closely followed by the hacker groups. In response to the WikiLeaks breach, Cyber Command was able to direct actions across the Department that quickly reduced risks to DoD information. These measures supported operational Commanders exercising their accountability for cybersecurity in their units.

I'd be pleased to give you more details on these events in closed session, and to tell you about still others that remain too sensitive to mention here.

I am proud of this record of success but aware that more needs to be done by Cyber Command as part of the larger cyber enterprise that includes the National Security Agency/Central Security Service (NSA/CSS), the Service cyber components, and the Defense Information Systems Agency (DISA). I foresee five challenges over the coming year that Cyber Command will face and continue to address. Those areas are the following:

1] Concept for Operating in Cyberspace: Every domain, by definition, has unique features that compel military operations in it to conform to its physical

or relational demands. Doctrine, tactics, techniques, and procedures have been under development for millennia in the land and maritime domains, for a century in the air domain, and for decades in space. In the cyber domain, however, we are just beginning to craft new doctrine and tactics, techniques, and procedures. At the strategic level, we are building our organizational structures to ensure we can deliver integrated cyber effects to support national and Combatant Commander requirements; we are developing doctrine for a pro-active, agile cyber force that can "maneuver" in cyberspace at the speed of the internet; and we are looking at the ways in which adversaries might seek to exploit our weaknesses. At the operational level, our objectives are to establish a single, integrated process to align Combatant Commanders' requirements with cyber capabilities; to develop functional emphases in the Service cyber components; and to draft a field manual or joint publication on cyber operations and demonstrate proof of concept for it. Finally, rapid deconfliction of operations is required, and that is garnering leadership attention as well. We are currently working closely with two of the geographic combatant commanders. Our goal is to ensure that a commander with a mission to execute has a full suite of cyber-assisted options from which to choose, and that he can understand what effects they will produce for him. Though we can only work such an intensive process with two of the combatant commanders at this time, we will be able to reach out eventually to all of the combatant commands.

2] Cybersecurity Responsibilities: Defending the nation in cyberspace requires a coordinated response among several key players from throughout the government. It takes a cross-government team to mature and implement an effective cyber strategy for the nation. From my perspective, there are three key players that make up this team:

- Department of Homeland Security – lead for coordinating the overall national effort to enhance the cybersecurity of U.S. critical infrastructure, and ensuring protection of the civilian federal government (.gov) networks and systems.
- Federal Bureau of Investigation (FBI) – responsible for detection, investigation, prevention, and response within the domestic arena under their authorities for law enforcement, domestic intelligence, counterintelligence, and counterterrorism. Importantly, when malicious cyber activity is detected in domestic space, the FBI takes the lead to prevent, investigate, and mitigate it.
- Department of Defense / Intelligence Community / NSA / Cyber Command – responsible for detection, prevention, and defense in foreign space, foreign cyber threat intelligence and attribution, security of national security and military systems; and, in extremis, defense of the homeland if the Nation comes under cyber attack from a full scope actor.

Cyber Command is working to ensure we have identified the roles and responsibilities correctly to accomplish our mission. Overall, our most pressing need across the government is to ensure we can see threats within our networks and thus address malware before it threatens us. Foundational to this is the information sharing that must go on between the federal government and the private sector, and within the private sector, while ensuring appropriate measures and oversight to protect privacy and preserve civil liberties. We welcome and support new statutory authorities for DHS that would ensure this information sharing takes place; an important reason why cyber legislation that promotes this sharing is so important to the nation. Finally, we are working within the Department and Administration on establishing the Rules of Engagement and criteria upon which Cyber Command will act. We are working with the Joint Staff to develop a decision

framework that allows us to identify threats and ensure senior leaders can share information rapidly and take action, if necessary.

3] Trained and Ready Force: At present we are critically short of the skills and the skilled people we as a Command and a nation require to manage our networks and protect U.S. interests in cyberspace. Our prosperity and our security now depend on a very skilled technical workforce, which is in high demand both in government and industry. We in DoD need to build a cyber workforce that can take action quickly across the full range of our mission sets as necessary. This will require us to adopt a single standard across the Department and the Services, so that we can truly operate as a single, joint force. In order to achieve our goals in this area by 2014, we must build a skilled force capable of full-spectrum cyber operations across a continuum of threats. We also need to build our workforce at Cyber Command and the Service Cyber Components so that, in extremis, we have the capability to defend the nation in cyberspace. We are reviewing recruitment and incentive programs in order to build and retain the best of the best cyber defenders, and we are working to standardize, track, and manage the training needed for all cyber personnel.

Let me mention one of the ways in which we are building the cyber force. Last fall we sponsored our first major tactical exercise, which we called CYBER FLAG (after the RED FLAG exercise that has trained generations of fighter pilots since the 1970s). This was a large, multi-day affair, in which operators from our Service cyber components engaged in realistic and intense simulated cyber combat against "live" opposition. This unprecedented exercise attracted a great deal of interest from senior leaders in the Pentagon and other departments and agencies, and dozens of observers attended its sessions. Nevertheless, CYBER FLAG was no mere drill, but a training exercise for those necessarily engaged in cyber operations now. The lessons that network

operators learned first-hand in CYBER FLAG are being applied daily in defense of our networks and in support of national policy goals.

4] Defensible Architecture: Our current information systems architecture in the Department of Defense was not built with security uppermost in mind, let alone with the idea of operationalizing it to enable military missions. Instead, we have seven million networked devices in 15,000 DoD network enclaves. Our vision is to fashion that architecture into an operational platform, not just a channel for communications and a place for data storage. To do so, our DoD cyber enterprise, with the Department's Chief Information Officers, DISA, and Cyber Command helping to lead the way, will build a common cloud infrastructure across the Department and the Services that will not only be more secure but more efficient—and ultimately less costly in this time of diminishing resources—than what we have today.

Cyber Command will directly benefit from this in its mission of directing the security, operation, and defense of DoD information systems. Our strategic objective is to reduce the attack surface of our critical networks that is available to adversaries, enabling us to "Defend and Jump" as needed. Our operational objectives are to reduce the number of network enclaves to the minimum possible; to implement a common cloud-based infrastructure to improve security across all of DoD; to move to a more secure model for data and services with better tagging and metadata; to implement identity-based access controls to services, as well as attribute-based access controls to control who can use those data; and finally to grow the capability to rapidly reconfigure the single network in response to mission requirements or enemy actions.

The NSA has begun making this vision a reality, with collateral benefits for Cyber Command in the process. The agency has sharply consolidated the number of desktop applications, closed half its help desks, trimmed the

number of data centers required, and saved money through corporate management of software licenses. Similar actions taken Department-wide will not only improve the security of the DoD's networks but also reduce its information technology costs, freeing money for other purposes and allowing for a re-dedication of cyber personnel to more urgent needs.

5] Global Visibility Enabling Action: We cannot wait for the implementation of that vision of a defensible architecture, however, to improve our situational awareness. Our commanders and our Services need to know what's happening inside and outside our networks, but at present we cannot even develop a definitive picture of the 15,000 DoD network enclaves and lack the capability to easily understand what is happening as it occurs. Furthermore, we must know in real time when and how the internet and the overall cyber environment inside and outside the United States are threatened in order to counter those threats. In this area, our strategic objectives are to enable unity of effort across DoD, the federal government, private partners and allied nations; to develop faster, more comprehensive, and timelier warning of threats against DoD networks and critical infrastructure; and to move beyond situational awareness to enabling integrated operational responses in cyberspace. Our operational objectives are to gain visibility of, and fuse information from, our own and public networks to enable action; to partner with the interagency, private infrastructure providers and global partners to share information; and to build capabilities to empower decision makers.

Cyber Command Major Accomplishments (March 2011 to March 2012)

Operational Impacts

Common Operating Picture (COP) Exercise: Cyber Command Joint Operations Center, the NSA/CSS Threat Operations Center and the DoD Cyber Crime Center participated in a White House-led National Level Exercise to test the

federal government's ability to develop a COP appropriate for White House-level consumers.

Cyber Training Advisory Council (CYTAC) Creation: The CYTAC is an advisory and coordination committee established to improve the quality, efficiency, and sufficiency of training for computer network defense, attack, and exploitation that will work to coordinate and standardize cyber training across all military services, Cyber Command, and NSA.

National Reconnaissance Office (NRO) War Game THOR'S HAMMER: Cyber Command personnel supported NRO's space and cyber wargame that increased the participant's understanding of critical space asset capabilities and their vulnerabilities to cyber attacks. Additionally, the wargame highlighted the interrelationship between space security and cyberspace security.

DHS National Cyber Incident Response Program: Synchronized DHS National Cyber Incident Response Program (NCIRP) with the DoD's Cyberspace Conditions alert system to facilitate future actions.

Global Cyber Synchronization Conference: Hosted the second Global Cyber Synchronization Conference on behalf of USSTRATCOM to integrate operational planning requirements across the combatant commands.

Policy and Doctrine

The Administration is working with the Congress to finalize cybersecurity legislation. Within the Administration, there is a strong and unified working relationship between DoD, DHS and NSA on cybersecurity matters; and NSA, NIST and DHS are closely partnered to address cybersecurity standards.

Senate Cybersecurity Exercise: Members of the Senate participated in a cybersecurity exercise on 7 March 2012 as the result of an all-Senate cybersecurity threat briefing given by the White House and Departmental Secretaries on 1 February 2012.

Support to Operations

Cyber Command Cyber Support Element (CSE) Placements: Working with the combatant commands to place a CSE at each COCOM tailored to their mission support requirements for cyberspace operations. Cyber Command has a full CSE deployed to USCENTCOM, a partial CSE to PACOM, and expects to deploy a CSE to USAFRICOM and USSOCOM within 6 months.

Cyber Command Force Management Workshop: The Cyber Command Force Management Workshop held in November brought together service cyber components to discuss Cyber Command support for the Combatant Commanders.

Trained and Ready Cyber Forces: Cyber Command, NSA and the military's cyber service components completed development of the Joint Cyberspace Training and Certification Standards (JCT&CS) document that will serve as the common foundation for training all cyber operators to unified standards across the DoD.

Enhancing Defenses

GLOBAL THUNDER 12: The Cyber Command Joint Operations Center (JOC) supported USSTRATCOM's annual Field Training Exercise (FTX) designed to validate our Nuclear Command Control Communications (NC3) OPLAN tasks. The JOC supported this FTX with reporting, analysis, conducting de-confliction, and responding to cyber related events.

Cyber Command Support to NIMBLE GHOST: Cyber Command worked with the Joint Staff for this DoD exercise to provide a forum for senior DoD leaders to examine policies and procedures that enable the defense of DoD critical U.S. networks and explore the department's ability to respond to a major cyberspace attack.

Building Team Cyber

DHS Blueprint for a Secure Cyber Future: Offered substantive comments in response to a review of DHS' draft Blueprint for a Secure Cyber Future; the Cybersecurity Strategy for the Homeland Security Enterprise.

Enhanced DHS and DoD Cybersecurity Operational Collaboration: Efforts remain underway by DHS and DoD to clarify responsibilities, assign specific actions, and establish timelines for implementing the DHS-DoD Joint Cybersecurity Vision in a cybersecurity work plan.

Tri-Lateral Defense Cyber Contact Group: Cyber Command and NSA personnel attended the Tri-Lateral Defense Cyber Contact Group (DCCG) completing a planning-focused tabletop exercise with the United Kingdom, Australia, USSTRATCOM, and OSD(P); used to develop a listing of issues that impede our ability to conduct cyberspace operations trilaterally.

Conclusion

We are working on all five of these focus areas simultaneously because they all demand our attention and because progress in each depends on progress in the others. Our capabilities across the board have to improve together, or good ideas in one area can be undermined by continuing weakness in another. We are moving with all deliberate speed, moreover, because the

American people will rightfully want results, not excuses, as we defend our nation.

In conclusion, allow me to thank you again for inviting me here to talk about the achievements and the plans of Cyber Command. Cyberspace provides both incredible opportunities and significant challenges for the Department of Defense and the nation. Cyber Command is part of a whole-of-government effort to capitalize on those opportunities, and to reduce and mitigate the uncertainties. With your continued support, I have no doubt that the hardworking and capable men and women of the Command will rise to those challenges and continue to make our nation proud of their accomplishments. And now I look forward to continuing this dialogue with you, both here and in the months ahead.

GEN Keith B. Alexander
United States Army

General Keith B. Alexander, USA, is the Commander, U.S. Cyber Command (USCYBERCOM) and Director, National Security Agency/Chief, Central Security Service (NSA/CSS), Fort George G. Meade, MD. As Commander, USCYBERCOM, he is responsible for planning, coordinating and conducting operations and defense of DoD computer networks as directed by USSTRATCOM. As the Director of NSA and Chief of CSS, he is responsible for a Department of Defense agency with national foreign intelligence, combat support, and U.S. national security information system protection responsibilities. NSA/CSS civilian and military personnel are stationed worldwide.

He was born in Syracuse, NY, and entered active duty at the U.S. Military Academy at West Point.

Previous assignments include the Deputy Chief of Staff (DCS, G-2), Headquarters, Department of the Army, Washington, DC; Commanding General of the U.S. Army Intelligence and Security Command at Fort Belvoir, VA; Director of Intelligence, United States Central Command, MacDill Air Force Base, FL.; and Deputy Director for Requirements, Capabilities, Assessments and Doctrine, J-2, for the Joint Chiefs of Staff. GEN Alexander has served in a variety of command assignments in Germany and the United States. These include tours as Commander of Border Field Office, 511th MI Battalion, 66th MI Group; 336th Army Security Agency Company, 525th MI Group; 204th MI Battalion; and 525th MI Brigade.

Additionally, GEN Alexander held key staff assignments as Deputy Director and Operations Officer, Army Intelligence Master Plan, for the Deputy Chief of Staff for Intelligence; S-3 and Executive Officer, 522nd MI Battalion, 2nd Armored Division; G-2 for the 1st Armored Division both in Germany and Operation DESERT SHIELD/DESERT STORM in Saudi Arabia.

GEN Alexander holds a Bachelor of Science degree from the U.S. Military Academy and a Master of Science degree in Business Administration from Boston University. He holds a Master of Science degree in Systems Technology (Electronic Warfare) and a Master of Science degree in Physics from the naval Post Graduate School. He also holds a Master of Science degree in National Security Strategy from the National Defense University. His military education includes the Armor Officer Basic Course, the Military Intelligence Officer Advanced Course, the U.S. Army Command and General Staff College, and the National War College.

His badges include the Senior Parachutist Badge, the Army Staff Identification Badge, and the Joint Chief of Staff Identification Badge.

ASD Creedon Testimony
HASC on Emerging Threats and Capabilities
March 20, 2012

Introduction

Thank you, Mr. Chairman and Ranking Member Langevin, for inviting the Department of Defense (DoD) to discuss our strategies and activities for addressing cyberspace challenges and opportunities. I am pleased to appear here today with Ms. Teri Takai, the DoD CIO, and General Keith Alexander, the Commander of U.S. Cyber Command. We are all here on behalf of the men and women of the Department who commit themselves every day to ensuring the safety of the United States, both at home and abroad.

Today I intend to present a brief overview of the Department's efforts in cyberspace, and I will provide an update on the implementation of the *Defense Strategy for Operating in Cyberspace* and the progress we have made in meeting the *Quadrennial Defense Review* and *Strategic Guidance* goals of operating effectively in cyberspace.

DoD continues to develop effective strategies for ensuring that the United States is prepared for all cyber contingencies across the entire spectrum from peace to crisis to war. Importantly, during these times of fiscal constraint, DoD is taking advantage of the efficiencies provided by advances in information technology.

Almost every feature of modern life now requires access to information infrastructure and DoD is no different. We maintain over 15,000 networks or enclaves and seven million computing devices in installations around the globe. The networks upon which the DoD relies represent both opportunities and challenges.

Looking forward, Secretary Panetta addressed the issue of cyber in his testimony to the House Armed Services Committee in October 2011 when he stated, "We continue to have to confront cyber attacks and the increasing number of those attacks that threaten us every day." We are considering increased spending on cyber over the next few years, even as we are planning significant cuts in other areas. Some particular areas where we may desire increases in the cyber budget might include:

- Increasing situational awareness tools and capabilities to monitor the security posture of DoD networks;
- Strengthening our ability to test capabilities and to operate effectively in a degraded environment; and
- Improving DoD support to the cybersecurity of the Defense Industrial Base and U.S. critical infrastructure, as appropriate.

Threats

These investments are critically important; they set the foundation for the Department's ability to face and defend against an ever-growing threat from malicious cyber actors. Whereas that threat was once the province of lone-wolf hackers, today, our nation, our businesses, and even our individual citizens are constantly targeted and exploited by an increasingly sophisticated set of actors. We believe the costs of these intrusions run into the billions of dollars annually and pose a clear threat to our economy and our security. Further, we are increasingly concerned about the threat to our Defense Industrial Base and the nation's critical infrastructure. We have seen the loss of significant amounts of intellectual property and sensitive Defense information that resides on or transits Defense Industrial Base systems. This

loss of key intellectual property has the potential to give an adversary leap-ahead technology to achieve parity with some of our most sensitive capabilities. As the recent report from the National Counterintelligence Executive shows, China conducts cyber-enabled economic espionage in order to shore up and support its military industries, thereby undermining the U.S. competitive edge in key technologies.

U.S critical infrastructure is increasingly vulnerable to cyber threats. DoD depends upon this infrastructure, including the electric grid, the telecommunications infrastructure, and key transportation systems, in order to function. Unless we as a nation do more to protect critical infrastructure assets and intellectual property, it is likely only a matter of time before we suffer a crippling blow that will greatly diminish DoD's ability to conduct our missions. DoD is ready to assist in this effort.

DoD's Actions

The Department has been working around the clock, often in close coordination with the Department of Homeland Security and other agencies, to protect the nation from these threats. Last July, DoD released the *Defense Strategy for Operating in Cyberspace* (DSOC). This strategy was a significant milestone for the Department because it was the first comprehensive strategy to address this new operational domain. The DSOC built upon the President's *National Security Strategy*, the *International Strategy for Cyberspace*, and the Department's *Quadrennial Defense Review*. The DSOC guides the Department's military, business, and intelligence activities in cyberspace to support of U.S. national security. Through five strategic initiatives, the DSOC lays out a framework to capitalize on the opportunities and address the threats created by cyberspace.

- First, DoD will treat cyberspace as an operational domain in order to organize, train, and equip our forces.
- Second, DoD will employ new operating concepts in order to protect DoD networks and systems.
- Third, DoD will partner with other departments and agencies, as well as the private sector, in order to enable a whole-of-government approach to cybersecurity.
- Fourth, DoD will build robust relationships with allies and international partners to strengthen our collective cybersecurity.
- Fifth and finally, DoD will leverage the nation's ingenuity by making more effective use of the cyber workforce and fostering rapid technological innovation.

DoD has made strides in each of these areas since the strategy was introduced nine months ago and established a governance body to manage the implementation of those initiatives. Co-chaired by the Under Secretary of Defense for Policy and the Director for Operations for the Joint Staff, the Cyber Integration Group assigns actions to appropriate components across OSD, the Joint Staff, the Services, the Combatant Commands, the Defense Cyber Crime Center, the National Security Agency, and the office of the Chief Information Officer. The accomplishments of this group attest to the progress we have made in addressing many of the issues regarding the new operational domain of cyberspace.

The Department is working with the Administration to update cyberspace operations policy, determine how we can better defend our critical infrastructure and intellectual property, and respond to advanced persistent threats. While we are responsible for protecting DoD's information systems and networks from cyber threats, the protection of infrastructure critical to national security requires the entire government's effort and extends to privately held

infrastructure owners. We are working closely with the Executive Branch Departments and Agencies on this significant challenge. Our recent Defense Industrial Base Cyber Pilot demonstrated that DoD could enhance the cybersecurity of Defense Industrial Base companies through a public-private cyber threat information sharing program.

Further, we are integrating cyber effects into our operational planning and addressing the policy issues constraining activity in this area. The Department is currently conducting a thorough review of the existing rules of engagement for cyberspace. We are also working closely with the Joint Staff on the implementation of a transitional command and control model for cyberspace operations. This interim framework will standardize existing organizational structures and command relationships across the Department to provide the full spectrum of cyberspace capabilities in response to the requirements of the President. The Joint Staff is also in the process of developing a Joint Publication for Cyberspace Operations. Although cyberspace operational doctrine already exists in various current publications, this will be the Department's first Joint Publication focused solely on cyberspace operations.

Also in line with our strategy and in accordance with the President's *International Strategy for Cyberspace*, DoD is developing a range of capabilities to protect the nation from our adversaries. The purpose of these capabilities is to provide the President with a full range of options to use in defending and securing our Nation in concert with the other elements of power we can bring to bear.

Within the U.S. government, DoD also works very closely with our colleagues in the Departments of Homeland Security, Justice, State, Treasury, Commerce, and others. Although DoD maintains robust and unique cyber capabilities that we use to defend our networks and the nation, we strongly believe in a whole-of-government approach to cybersecurity. As such, we

fully support the Department of Homeland Security's role coordinating the overall national effort to enhance the cybersecurity of U.S. critical infrastructure.

One example of interagency collaboration is the former Defense Industrial Base Cyber Pilot, now known as the Joint Cybersecurity Services Pilot. Based initially on the Defense Industrial Base Cybersecurity and Information Assurance Program that is run by the DoD Chief Information Officer, DoD and Homeland Security established an information sharing construct with Commercial Service Providers to provide managed security services enhanced by government threat information to Defense Industrial Base companies. In partnership with Homeland Security, we are working together on plans make it a permanent program for the Defense Industrial Base.

Finally, we are working closely with our interagency partners to address the vulnerabilities represented by the supply chain of critical equipment upon which our networks and systems rely. DoD serves as a co-lead on a supply chain risk management task force that was established a year ago and we are making progress in addressing the requirement for a secure and trusted manufacturing environment.

Beyond the U.S. government, DoD is also working with our interagency partners and the private sector to improve security and foster innovation, while ensuring an open, accessible and private sector-owned Internet. We understand that building strong partnerships with industry is essential to our collective security. An important initiative in this area is the Enduring Security Framework, which provides a mechanism for Homeland Security, DoD, and the Director of National Intelligence to work with key industry leaders on cybersecurity issues that affect both the private sector and defense and government networks.

On the international front, DoD is pursuing both bilateral and multilateral engagements. First, we are collaborating with our close allies such as the United Kingdom, Australia, Canada, Japan, and the North Atlantic Treaty Organization on improving international cybersecurity. We are also working closely with the Department of State to develop international norms of behavior that will serve to guide our international partnerships. If international norms of behavior in cyberspace could be achieved, adherence to such norms would bring a level of predictability to state conduct and help prevent the misunderstandings that could lead to conflict. In addition, DoD also participates and interacts with the various Internet governance institutions to ensure that the Internet remains open, interoperable, secure, and reliable.

In addition to the increasing threats we face through cyberspace, one of the challenges is the lack of clear authorities for providing for the cybersecurity of U.S. critical infrastructure. Although the Department does not require any additional authorities in cyberspace for Defense missions, we do support providing additional authorities to the Department of Homeland Security, including the authority to establish, in consultation with the other agencies of the government, risk-performance standards for core critical information infrastructure to ensure a baseline level of security

Another challenge is to balance the nation's need for cybersecurity with privacy and civil liberties. In this area, DoD is committed to focusing on external actors while ensuring the privacy and civil liberties of our citizens in our efforts to support the cybersecurity of U.S. critical infrastructure.

Conclusion

Thank you for this opportunity to describe some of the opportunities and challenges that DoD faces in cyberspace. These lines of effort represent significant investments in our nation's defense and reflect the high priority that Secretary Panetta places on cybersecurity. DoD is working hard to ensure our nation's security, but there is still more work to be done.

We fully support Congressional efforts to provide the Department of Homeland Security, as our partner and domestic lead for cybersecurity, with the authorities and resources it needs. We also believe that Homeland Security should have the authority to designate core critical infrastructure and establish baseline risk-based performance standards for cybersecurity. Additionally, we must do more to encourage information sharing in a way that maintains the Administration's focus on the maintenance of privacy and civil liberties. These reforms would go a long way to keeping our nation ahead of the evolving threat while protecting our basic values. With the help of and partnership with Congress, DoD is working hard to protect our nation and to provide the necessary capabilities to keep our country safe.

Madelyn R. Creedon

Assistant Secretary for Global Strategic Affairs (GSA)

Madelyn Creedon was confirmed by the U.S. Senate as the Assistant Secretary of Defense for Global Strategic Affairs (GSA) on August 2, 2011. In this capacity she supports the Under Secretary of Defense for Policy in overseeing policy development and execution in the areas of countering Weapons of Mass Destruction (WMD), U.S. nuclear forces and missile defense, and DOD cyber security and space issues.

Prior to her confirmation, Ms. Creedon was counsel for the Democratic staff on the Senate Committee on Armed Services and was responsible for the Subcommittee on Strategic Forces as well as threat reduction and nuclear nonproliferation issues.

In 2000, she left the Armed Services Committee to become the Deputy Administrator for Defense Programs at the National Nuclear Security Administration, Department of Energy (DOE), and returned to the Committee in January 2001.

Prior to joining the Armed Services Committee staff in March 1997, she was the Associate Deputy Secretary of Energy for National Security Programs at the Department of Energy, beginning in October 1995.

From November 1994 through October 1995, Ms. Creedon was the General Counsel for the Defense Base Closure and Realignment Commission. This Commission, under the Chairmanship of former Senator Alan Dixon of Illinois, was responsible for recommending to the President military bases for closure or realignment.

From 1990 through November 1994, Ms. Creedon was counsel for the Senate Committee on Armed Services, under the Chairmanship of Senator Sam Nunn. While on the committee staff she was responsible for DOE national security programs, DOE and DOD environmental programs, and base closure transition and implementation programs.

Before joining the staff of the Senate Armed Services committee, Ms. Creedon was a trial attorney and Acting Assistant General Counsel for special litigation with the DOE Office of the General Counsel for 10 years.

Born and raised in Indianapolis, Indiana, Ms. Creedon is a graduate of St. Louis University School of Law, where she was captain of the moot court team. Her undergraduate degree is in political science from the University of Evansville, Evansville, Indiana.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 20, 2012

QUESTIONS SUBMITTED BY MR. LANGEVIN

Mr. LANGEVIN. Are you confident in the state of the career paths for cyber professionals, and do you feel that your recruiting, retention, and career progression needs are being adequately addressed?

Ms. TAKAI. In light of emerging cyber threats, cyber workforce roles, responsibilities and skill requirements continue to evolve, not only in, but across the Federal Government and industry. DOD is working with the Federal Government through the National Initiative for Cybersecurity Education (NICE) and Federal CIO Council to identify current and forthcoming cyber skill requirements, define career paths for cyber professionals, and to determine the optimal courses of action to ensure a pipeline of cyber professionals is available to meet mission mandates. These efforts may result in new requirements and methodologies in the recruitment, retention and career management of the Department's cyber workforce.

Currently, several strategies are in place to aid in recruiting and retaining a skilled cyber workforce. Federal direct-hire authority provides with flexibility in recruiting and hiring select information security (cybersecurity) personnel within the civilian IT Management series. DOD also has Schedule A hiring authority for select cybersecurity positions for certain IT and non-IT civilian job series; the Department is working with the Office of Personnel Management (OPM) to extend and enhance this authority as it expires in December 2012. DOD uses the Information Assurance Scholarship Program (IASP) to attract students from top universities and colleges, and to retain personnel with cyber and information assurance skill sets who wish to further their education. In addition, CIO oversees the Information Resources Management College (iCollege) of the National Defense University, which recently introduced a Cyber Leadership Program. These authorities and programs, along with military recruiting and retention bonuses, are currently used to recruit and retain cyber personnel and are essential to maintaining the health of this community.

Mr. LANGEVIN. How is DOD capturing lessons learned from real-world cyber events and major exercises?

Ms. TAKAI. Real world lessons learned are submitted to the Joint Lessons Learned Information System (JLLIS) database system of record. JLLIS is the system of record for Lessons Learned. Typically, they are communicated in the form of Situational Awareness Reports (SARs). For certain major events, a detailed analysis of the incident is conducted and with the results published as an SAR, which details the incident, threat tactics, techniques and procedures, as well as countermeasures/mitigation options. Lesser events are often documented in quarterly SARs that show trends, common TTPs, systemic issues, etc. Exercise lessons learned also are inputted into JLLIS and their capture in the database has greatly improved over the last 12 to 18 months. Anyone with SIPR access may request an account to access JLLIS content.

In addition to JLLIS, the Military Departments track major events via their respective database systems. For example, Army Computer Network Defense (CND) events are tracked in ACID, the Army CND Incident Database. The Navy Lessons Learned System (NLLS) is the Navy's process for collection and dissemination of significant lessons learned, summary reports and port visit reports from maritime operations, exercises and other events.

Mr. LANGEVIN. What more can be done to engage our allies, especially NATO? How can we leverage DOD "building partnership capacity" authorities to train and equip foreign forces to improve our allies' capabilities related to cyber operations?

Ms. TAKAI. We are engaging our key allies and partners, including NATO, through agreements to share unclassified and classified cyber defense information. We may be able to do more by focusing on producing more classified cyber defense information which is releasable to these allies and partners. We are leveraging theater security cooperation programs in the Geographic Combatant Commands by including "building cyber defense capacity" with focused on treaty allies and priority partner nations. This effort is led in the CIO by our International Cyber Security Program and coordinated with the Geographic Combatant Command, Joint Staff and OSD Policy. Initially this generally consists of training all levels of cyber leadership and practitioners in cyber defense best practices. This should establish an inci-

dent response capability (e.g. a CERT) with the appropriate policies in place to govern network operations and cyber defense. This may evolve into greater information sharing and potentially exercises once a capability is developed. Additionally CIO semi-annually hosts an international cyber defense workshop to provide a week long virtual training workshop to over twenty nations. We regularly invite more than forty nations to the workshop and usually have 25 or more participate.

Mr. LANGEVIN. What discussions and actions are going on within NATO to improve the capabilities of the alliance to deal with cyber threats?

Ms. TAKAI. NATO developed a new cyber defense concept in March 2011, a new Cyber Defense Policy in June 2011 and from that policy a cyber defense action plan to improve NATO's internal cyber defense capability as a priority, additionally providing advice or assistance to nations that request assistance. The current actions are a recently awarded contract (58m Euro) to enhance the NATO Computer Incident Response Capability and ongoing actions to monitor that project. Ongoing discussions focus on developing a methodology for national information systems that support NATO missions to be identified and provided minimum cyber defense standards. Further parts of the enhanced capability in the cyber defense action plan are the development of training and exercises for NATO nations, providing minimum standards for cyber defense for nations, and developing rapid reaction teams to assist nations when facing significant cyber incidents. Further possible enhancements are also under discussion but the current main focus is on ensuring the ongoing project is closely monitored for adherence to timelines and completing the full package of enhanced sensors and systems for cyber defense. These ongoing efforts are regularly reviewed by CIO's International Cyber Security Program.

Mr. LANGEVIN. What is the status of development and delivery of proposed National Cyber Range capabilities? Are resources adequate to continue maturing range capabilities?

Ms. TAKAI. The goal of the DARPA NCR program is to develop the architecture and software tools for a secure test facility that can rapidly emulate the complexity of defense and commercial networks, allowing for cost-effective and timely validation of cyber technologies.

The program has completed the technical design and all major software development. The developed architecture and tools are being demonstrated at scale on a prototype facility. The NCR software includes extensive experiment design tools, an automated range build-out capability, real-time data visualization tools, and automated range sanitization. The demonstration facility is currently accredited for operation from Unclassified to Top Secret/Special Access Program level and is capable of supporting simultaneous testing at multiple security levels. Special Compartmentalized Information accreditation is currently being pursued.

To date, there have been two completed tests (December 2011 and January 2012). Both tests showed the ability to setup the range in a day, test for multiple days (each test was at a different classification level), and then tear the range down and sanitize it in a day. Eight additional tests are currently being planned and scheduled.

The Department is planning a series of events on the NCR with Joint Information Operations Range (JIOR), and Cyber Range also participating to stress NCR and other range capabilities, identify what is mature, what is not, and characterize the magnitude of gaps that will need to be addressed for adequate testing and evaluation, training and exercise capability.

Mr. LANGEVIN. What CYBERCOM capabilities are in need of further development to address our national vulnerabilities in cyberspace?

General ALEXANDER. Our desired end state is to maintain and preserve the U.S. freedom of access to allow maneuver in cyberspace while supporting the same for our allies and partners. To do this, it is essential to:

- Develop capabilities to support Indications and Warning (I&W) of attacks in cyberspace
- Develop integrated Command and Control for seamless transition from defensive to offensive posture
- Develop integrated situational awareness capability to sense, support real time maneuver, and engagement in cyberspace
- Develop capability for training, testing, and effects prediction for cyber capabilities
- Enhanced analytic and target development capabilities
- Development of integrated architectures and frameworks to support network resiliency and maneuver in cyberspace especially in contested and congested networks

Mr. LANGEVIN. Since the signing of the Memorandum of Understanding between DOD and DHS, what activities have the two organizations been carrying out under that MOU?

General ALEXANDER. The implementation of the MOU has resulted in the creation of a Fort Meade-based office for the DHS–DOD Joint Coordination Element (JCE), co-lead by DHS and DOD seniors. Activated in December 2010, the JCE now comprises 16 full-time personnel from DHS and DOD and is focused on achieving cross-departmental "unity of effort" in cyberspace operations. The ultimate goal is to enable the USG to agilely perform integrated operational response in all areas in which the adversary pursues malicious activity—with the benefit of robust shared situational awareness.

The JCE is creating enduring relationships and process improvements across the two Departments. In its first year, the JCE initiated a number of major activities designed to enable these goals, by successfully bridging the gap between policy and operations. A few examples include:

- Congress directed DHS and DOD to draft a Joint Cybersecurity Pilot Plan. This plan was penned by the JCE, signed by both Departments, and transmitted to the Committees on Appropriations in August 2011.
- The JCE is defining cross-department command and control/unity of effort models to enable agile, effective, and timely operations.
- The JCE is defining the discrete and complementary function of the major DHS and DOD operational organization to achieve harmonization of major DHS and DOD operational elements.
- As an outgrowth of the Defense Industrial Base (DIB) Cybersecurity "opt in" Pilot, Department seniors have agreed on a framework to create government-enabled Managed Security Services to address advanced threats targeting the nation. The JCE has drafted detailed plans to support this effort with an eye toward scalable solutions.

Mr. LANGEVIN. Are you confident in the state of the career paths for cyber professionals, and do you feel that your recruiting, retention, and career progression needs are being adequately addressed?

General ALEXANDER. There has been a great deal of work done in developing career paths for cyber professionals. The pace at which we are developing cyber professionals is challenged by the demand for skilled personnel (in both government and in the private sector) to keep pace with rapidly advancing technology. At USCYBERCOM we have made recent, significant strides into defining and advising what those career paths should include. One of the biggest challenges to "operationalizing" activities in this domain is the development of the cyber workforce. The major cultural shift within the military has momentum; however, codifying and teaching the required skills in such a dynamic, ever-evolving domain, is a challenge. We are confident that our activities have laid a solid foundation for cyber professional career paths. Examples of our ongoing efforts follow.

Joint Cyberspace Training and Certification Standards (JCT&CS). The JCT&CS provides an overarching framework for the Services, if they so choose, for training for the current and future cyberspace workforce over their careers. JCT&CS advises nearly every aspect of individual force training and education and follows the Joint Training System model for methodology. The standards outlined in JCT&CS inform curriculum, certification, and other standards used to effectively train forces to meet the ever-evolving warfighter demands of the cyberspace domain. Based on the current lack of policy on cyber training, the Services use of these standards is voluntary at this time.

Assessment and Recruiting. Initial assessment and recruiting to identify the best candidates possible to support the cyberspace mission is critical. The JCT&CS provides key insights into the preliminary knowledge, skills, and abilities needed to ensure success. Service recruiting efforts will be advised of these standards and special screening techniques and evaluations will be developed to identify suitable candidates. In addition, the newness of this command and our challenging mission appears to be a draw for talented personnel. We anticipate the competition for cyber talent to become more intense and we must be enabled to respond rapidly with appropriate DOD recruiting/retention policies and incentives. Delays in recruiting and retaining cyber talent could adversely affect the command's operational capability in the future. Against our current authorizations, our civilian fill rate is adequate. However, to efficiently operate as a Sub-Unified Command we estimate an additional need of approximately 500 billets. Moreover, we expect competition for future talent to intensify, affecting initial hires and retention. To address the anticipated challenges in the short-term, we are collaborating with United States Strategic Command and the Office of the Secretary of Defense to permanently extend the temporary hiring authorities granted to us (e.g. Schedule A- which is set to expire

Dec '12). Long-term, we are advocating for: special salary rates, tuition reimbursement, access to specialized training and robust professional development opportunities as incentives for potential employees and to retain them once they have been hired. Underlying all of these initiatives, we support the development of separate cyber operations/planner career fields for our civilian and military personnel.

Service School Qualification Training. The Services currently provide for both enlisted and officers, basic entry training for their respective skills. For many cryptologic skills today that instruction is provided through Joint Cyber Analysis Course at Corry Station in Florida. As a backdrop, the JCT&CS will provide guidance through curriculum advisory messages in curriculum development, advising the Services on the Knowledge, Skills and Abilities (KSAs) with metrics to ensure success for those whose assignments require the ability to perform in one or multiple cyber work roles.

Professional and Continuing Education. Once the basic schooling is completed, Service military and civilians continue to work to sharpen skills and capabilities through professional and continuing education. For the Joint community, this includes Joint Individual training and for IA professionals, training and certification is completed in compliance with prevailing DOD policy (DOD Directive 8570.01M). Again, the JCT&CS provides a broad framework to inform joint and Service training for cyberspace KSAs. An aggressive and effective retention and career feedback process is permeated throughout the careers of the cyberspace workforce. Constant inputs to training value, curriculum development, and career utilization will be used to advise senior leadership on job satisfaction and how well training enables the workforce to be successful in their assignments. Key to the success of this program is the agility at which the joint training standards can be modified and those changes permeated through professional and continuing education to keep the DOD cyberspace workforce in the forefront globally.

Collective Training. Even with a robust individual training program, individuals fight as crews, staffs, and organizations. The training spectrum includes an aggressive collective training program that trains, certifies, and then exercises the future cyberspace workforce. Training and certification guidelines are contained in the JCT&CS. Methods and modes are under development to measure the ability of crews, staffs, and organizations to meet the demands of fighting and winning in the cyberspace domain. Ultimately, this training is tested in cyberspace exercise events that focus on cyberspace operations with objectives that tie back to Joint Mission Essential Tasks. Today, at the tactical level, we've developed Cyber Flag, currently an annual event, that brings together the Service's cyber operators to defend and fight against a cunning, realistic aggressor. This environment allows us to understand the ability of our Service component teams and ultimately, our ability to perform essential missions.

Mr. LANGEVIN. Do you feel that the command structure for integrating non-kinetic effects from cyber into the battlespace is adequately defined?

General ALEXANDER. The command structure for integrating non-kinetic effects into joint operations is adequately defined, but the Department continues to develop and improve its implementation. Through the refinement of joint doctrine, planning, and procedures, we have put in place a number of mechanisms to integrate kinetic and non-kinetic effects.

We have long recognized the need for cyberspace doctrine that can address the unique attributes of cyberspace, the interdependencies with the land, air, sea, and space domains, and provide a model command structure to build upon.

The cyberspace operational planning process is aligned with joint doctrine, which has been developed and battle-tested over time as the preferred way for combatant commanders to plan, synchronize, de-conflict, and conduct operations. We have successfully adapted this process for cyberspace and have exercised it a number of times with the combatant commands to validate its applicability. Likewise, these exercises have helped us refine our command and control (C2) model to support the integration of cyberspace operations with other Combatant Command operations.

Mr. LANGEVIN. Can you briefly describe how CYBERCOM supports joint training efforts for inter-service missions?

General ALEXANDER. USCYBERCOM works with Service Component, Joint Staff and Agency training leads to collaborate on processes for continued development/refinement of DOD cyberspace training and certification standards. We have developed relationships with appropriate stakeholders including Service HQ, Combat Support Agencies, public and private academic institutions, and Joint and Service training and education activities. We support efforts to draft and staff policy that identifies roles, responsibilities, and processes as well as ensures consistency with other policy/guidance documentation in order to support joint training efforts DOD-wide. The Joint Cyberspace Training and Certification Standards (JCT&CS) pro-

vides an overarching framework for the Services, if they so choose, for training for the current and future cyberspace workforce over their careers. JCT&CS advises nearly every aspect of individual force training and education and follows the Joint Training System model for methodology. Our intent is to execute policy within national and military guidance in coordination with stakeholders and Communities of Interest to promulgate common training and certification standards.

Additionally, USCYBERCOM supports the Combatant Commands exercise of their warplans via Tier 1 Exercises. USCYBERCOM and its Service components provide planning and operations expertise to meet the exercise/training objectives. For FY12, USCYBERCOM is directly supporting or involved with 17 joint exercises, and is planning CYBERFLAG–12. Priority of support resides with National level, USCENTCOM, USPACOM, and USEUCOM exercises.

Mr. LANGEVIN. What more can be done to engage our allies, especially NATO? How can we leverage DOD "building partnership capacity" authorities to train and equip foreign forces to improve our allies' capabilities related to cyber operations?

General ALEXANDER. First, the United States can increase information and cyber capability sharing by developing and sharing cyber hygiene "best practices," sharing cyber threat information, and providing cybersecurity tools. Second, the United States can conduct tabletop exercises to identify legal and policy constraints and "live" exercises to build shared situational awareness and interoperability. Third, the United States can enhance education and training through congressional programs to allow foreign military officers to attend training in the United States and host or co-host conferences or seminars on cybersecurity. Fourth, the United States can expand the State Partnership Program to link more National Guard Cyber Warfare units with partner nations to increase engagement and training opportunities.

USCYBERCOM has shared portions of the methodology in developing Joint Cyberspace Training and Certification Standards (JCT&CS) for the command's cyber workforce and the workforce of the Service Cyber Components that are under operational control of the Commander. USCYBERCOM has also developed and manages several training courses that contribute to the professionalization of the cyber workforce (i.e. Joint Advanced Cyber Warfare Course–JACWC, Joint Cyberspace Operational Planners Course Mobile Training Team JCOPC MTT). The USCYBERCOM Joint Exercises and Training Directorate developed a version of JACWC (Joint Advanced Cyber Engagement Series–JACES) that is releasable to our allies, and is currently developing a similarly releasable version of JCOPC at the request of EUCOM and AFRICOM. The first session of JACES with 33 key partner nation students concluded 20 April 2012. USCYBERCOMs intent is to continue to build key partner relationships by sharing releasable components of its workforce development efforts.

Mr. LANGEVIN. What discussions and actions are going on within NATO to improve the capabilities of the alliance to deal with cyber threats?

General ALEXANDER. NATO has been actively working to improve the Alliance's capabilities to deal with cyber threats. A NATO Policy on cyber defense was recently approved and focuses on preventing cyber attacks and building resilience. The policy is being implemented via an action plan, which includes the NATO Computer Incident Response Capability (NCIRC) achieving full operational capability by the end of 2012. U.S. European Command is a key enabler and provides support to the NCIRC. Additionally, the United States is encouraging NATO to fully integrate cyberspace operations into planning, exercises, training, and education. Lastly, the United States is educating NATO on lessons learned from the Government's realignment to meet cybersecurity goals and the organizational and command and control structure of U.S. Cyber Command and other U.S. Government cyber units to influence NATO's civilian and military command structure development.

At USCYBERCOM, we have participated in the annual NATO cyber exercise Cyber Coalition. This is a NATO event facilitating the improvement and development of coherent procedures and mechanisms for cyber defense; exercise strategic decision-making procedures, technical and operational procedures, and collaboration between all participants, including the private and public sectors.

Several of our NATO allies are participating in the planning for Cyber Flag 13–1. The eight-day exercise schedule consists of four days with allies and the remaining four days as U.S. only due to classification considerations. Coalition partners will be invited to participate in future Cyber Flag exercises in order to build capacities and further enable partnership opportunities.

Mr. LANGEVIN. Are you confident in the state of the career paths for cyber professionals, and do you feel that your recruiting, retention, and career progression needs are being adequately addressed?

Secretary CREEDON. In light of emerging cyber threats, cyber workforce roles, responsibilities and skill requirements continue to evolve, not only in DOD, but across

the Federal Government and industry. DOD is working with the Federal Government through the National Initiative for Cybersecurity Education (NICE) and Federal CIO Council to identify current and forthcoming cyber skill requirements, define career paths for cyber professionals, and determine the optimal courses of action to ensure a pipeline of cyber professionals is available to meet mission mandates. These efforts may result in new requirements and methodologies in the recruitment, retention and career management of the Department's cyber workforce.

Currently, several strategies are in place to aid in recruiting and retaining a skilled cyber workforce. Federal direct-hire authority provides with flexibility in recruiting and hiring select information security (cybersecurity) personnel within the civilian IT Management series. DOD also has Schedule A hiring authority for select cybersecurity positions for certain IT and non-IT civilian job series; the Department is working with the Office of Personnel Management to extend and enhance this authority as it expires in December 2012. DOD uses the Information Assurance Scholarship Program (IASP) to attract students from top universities and colleges, and to retain personnel with cyber and information assurance skill sets who wish to further their education. In addition, CIO oversees the Information Resources Management College (iCollege) of the National Defense University, which recently introduced a Cyber Leadership Program. These authorities and programs, along with military recruiting and retention bonuses, are currently used to recruit and retain cyber personnel and are essential to maintaining the health of this community.

Mr. LANGEVIN. How is DOD capturing lessons learned from real-world cyber events and major exercises?

Secretary CREEDON. Real-world and exercise cyber lessons learned are submitted to the Joint Lessons Learned Information System (JLLIS) database system of record. JLLIS is the system of record for Lessons Learned. Typically, they are communicated in the form of Situational Awareness Reports (SARs). For certain major events U.S. Cyber Command conducts detailed analysis of the incident and then publishes the result as an SAR, which details the incident; threat tactics, techniques and procedures; as well as countermeasures/mitigation options. Lesser events are often documented in quarterly SARs that show trends, common TTPs, and systemic issues. Exercise lessons learned also are input to JLLIS and their capture in the database has greatly improved over the last 12 to 18 months. Anyone with SIPR access may request an account to access JLLIS content.

In addition to JLLIS, the Services also track major events via their respective database systems. For example, Army computer network defense (CND) events are tracked in ACID, the Army CND Incident Database. The Navy Lessons Learned System (NLLS) is the Navy's process for collection and dissemination of significant lessons learned, summary reports and port visit reports from maritime operations, exercises and other events.

Mr. LANGEVIN. What more can be done to engage our allies, especially NATO? How can we leverage DOD "building partnership capacity" authorities to train and equip foreign forces to improve our allies' capabilities related to cyber operations?

Secretary CREEDON. The Department's authorities to build the security capacity of our foreign partners can be useful tools that contribute significantly to a variety of missions, from counterterrorism and combating weapons of mass destruction, to stability and counterinsurgency operations. For cyber operations there are no current plans to use these specific authorities; rather the Department works collaboratively with NATO and other allies.

Our NATO allies recognize the increasing importance of cyber defense, as demonstrated by the 2010 Lisbon Summit Declaration, NATO's revised Strategic Concept, and the issuance of a revised NATO Policy on Cyber Defense in June of 2011. We are actively engaged in working with our NATO allies to ensure their continued commitment to NATO's new policy and the steps outlined in its Action Plan. More broadly, through our Geographic Combatant Commands, we are exploring ways in which we can work more closely with allies and partners to help them improve their cyber security and ensure that they are investing in enhanced security for their national networks. This is also an area where we are working closely with the Departments of State, Homeland Security, and other key USG stakeholders

Mr. LANGEVIN. What discussions and actions are going on within NATO to improve the capabilities of the alliance to deal with cyber threats?

Secretary CREEDON. Beginning with the 2010 Lisbon Summit Declaration and followed by NATO's revised Strategic Concept in which the protection of the Alliance's information systems was made a priority task, the U.S. Department of Defense has been actively engaged in working with NATO to improve the Alliance's ability to defend against the ever growing cyber threats.

In addition, last year NATO Defense Ministers approved a revised NATO Policy on cyber defense. The policy offers a coordinated approach to cyber defense across

the Alliance and focuses on preventing cyber attacks and building resilience. The new policy is currently being implemented through an Action Plan that has a number of elements, but the most important is achieving NATO Computer Incident Response Capability (NCIRC) full operational capability by the end of 2012. By bringing all of NATO organizations' networks under NCIRC authority and protection, the NCIRC will significantly increase the Alliance's ability to defend and recover in the event of a cyber attack against systems of critical importance to the Alliance. Implementation is on track and the U.S. Department of Defense will continue to strongly support NATO's efforts in this area.

QUESTIONS SUBMITTED BY MR. FRANKS

Mr. FRANKS. With respect to defense installations within the United States, how reliant are our IT and cybersecurity systems on the supply of stable, reliable, and uninterrupted electricity from the civilian power grid, and how prepared are we to carry out the defense mission if the power grid or a substantial part of it were to go down for extended period, for example: two weeks or longer due to severe space weather or man-made electromagnetic pulse?

General ALEXANDER. Defense installations themselves typically have means to provide backup power for various durations. Additionally, DOD typically contracts with multiple vendors for connectivity to minimize the number of single points of failure. However, a great deal of DOD's cyberspace is served by and through commercial providers. The degree to which these commercial providers—and the companies upon which they rely—can sustain operations in the event of an extended power outage varies considerably. We are aware that such dependencies exist and are actively working to identify just those kinds of critical infrastructures and key resources as part of a larger strategy to ensure robust cyber defense of the ".com" and ".gov" portions of cyberspace that DOD relies upon for mission readiness.

Mr. FRANKS. How confident are you that the private power industry is prepared to resist and defeat cyber attacks against its control and power distribution systems and are there approaches we can take with industry that don't involve burdening industry with unnecessary regulation, to assist industry to protect this vital infrastructure and ensure that defense-related IT and cybersecurity systems are not degraded or rendered useless by an extended period of time without electricity?

Secretary CREEDON. Commercial power sources continue to be threatened by a wide array of threats. Commercial electric power providers rely on Industrial Control Systems (ICS) to control and operate the power grid and, due to potential vulnerabilities with these systems, scenarios exist where malicious actors could gain control of critical components. Today's threat environment is dynamic and, as a result, organizations must be vigilant and adaptable in monitoring systems and implementing controls in response to current threats.

DOD conducts ongoing analysis and partners with multiple entities including the Department of Energy (DOE), Department of Homeland Security (DHS), the commercial ICS community, and the Federal Energy Regulatory Commission to stay abreast of the threat and better assess industry preparedness. DOD, along with its interagency and industry partners, is moving in a deliberate and aggressive fashion to close the gaps associated with energy surety.

In addition, DOE, and DHS recently launched the Energy Surety Public Private Partnership to better understand and improve the surety of energy infrastructure supporting national security missions. DOD is also participating in an effort led by DOE to develop a cybersecurity maturity model focused on managing dynamic threats to the grid and evaluating cybersecurity capabilities. Finally, there are other efforts underway focused on awareness and managing the threats to the grid such as the North American Electric Reliability Corporation cyber attack task force and a public/private collaborative effort to develop risk management guidelines. We believe these efforts will accomplish a great deal in managing the threat to our power sector