[H.A.S.C. No. 113–17]

INFORMATION TECHNOLOGY AND CYBER OPERATIONS: MODERNIZATION AND POLICY ISSUES TO SUPPORT THE FUTURE FORCE

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

HEARING HELD
MARCH 13, 2013

U.S. GOVERNMENT PRINTING OFFICE
80–187 WASHINGTON : 2013

SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES

MAC THORNBERRY, Texas, *Chairman*

JEFF MILLER, Florida
JOHN KLINE, Minnesota
BILL SHUSTER, Pennsylvania
RICHARD B. NUGENT, Florida
TRENT FRANKS, Arizona
DUNCAN HUNTER, California
CHRISTOPHER P. GIBSON, New York
VICKY HARTZLER, Missouri
JOSEPH J. HECK, Nevada

JAMES R. LANGEVIN, Rhode Island
SUSAN A. DAVIS, California
HENRY C. "HANK" JOHNSON, JR., Georgia
ANDRÉ CARSON, Indiana
DANIEL B. MAFFEI, New York
DEREK KILMER, Washington
JOAQUIN CASTRO, Texas
SCOTT H. PETERS, California

KEVIN GATES, *Professional Staff Member*
TIM MCCLEES, *Professional Staff Member*
JULIE HERBERT, *Clerk*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2013

WEDNESDAY, MARCH 13, 2013

INFORMATION TECHNOLOGY AND CYBER OPERATIONS: MODERNIZATION AND POLICY ISSUES TO SUPPORT THE FUTURE FORCE

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

INFORMATION TECHNOLOGY AND CYBER OPERATIONS: MODERNIZATION AND POLICY ISSUES TO SUPPORT THE FUTURE FORCE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES,
Washington, DC, Wednesday, March 13, 2013.

The subcommittee met, pursuant to call, at 3:46 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 INTELLIGENCE, EMERGING THREATS AND CAPABILITIES

Mr. THORNBERRY. The subcommittee hearing will come to order. I appreciate our witnesses and guests and their patience. There are some days that just don't work very well, and this is certainly one of them.

I will ask unanimous consent to put my opening statement in the record and yield to the gentleman from Rhode Island for any comments he would like to make.

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

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank our witnesses for appearing before the subcommittee today. This is obviously an important hearing as our national security is dependent on our information systems, and those networks are critical to all aspects of our defense. Yet, one only needs to look at recent headlines, even of the day, to understand the unrelenting and sophisticated threats that we face in the cyber domain.

Now we continue to see just how vulnerable such networks are in other sectors of our society, at a potential cost of billions lost to cybercrime, and we know our defense networks are at even greater risk. So obviously, though, they must be fail-proof and secure.

Now we are still waiting for this year's budget, but I believe it is safe to say that IT [information technology] represents a large piece, $33 billion last year for that matter, and that is a significant figure. And we must be ever mindful of our responsibility to make the most effective use of taxpayer's investments in these capabilities.

Now we are aware that the Department has experienced some challenges in acquiring certain IT systems and services in the past. So today, I would like to hear what steps we are taking to tackle those challenges in order to get the connectivity we need at a reasonable price.

DOD [Department of Defense] cyber operations are quite literally a growth business, and it is one of the rare portions of the DOD that will be growing indefinitely into the future; and there have been significant developments in just one year since our last posture hearing.

Now we are starting to get answers to some of the questions about how and when the United States might conduct the full range of military cyber activities, and I would like to discuss that today to the extent that this forum allows.

And I understand that Cyber Command [CYBERCOM] is beginning to organize itself into mission teams, which is an exciting step. But the manpower cost is enormous and the education and training requirement significant. This is going to take, obviously, a lot of work to get right.

I would be greatly interested to hear how, to hear our panelists' thoughts on how we refine the education, recruitment, retention and training of the highly specialized personnel that we need. And I would also like to hear how CYBERCOM is interfacing with combatant commanders to provide its unique capabilities wherever and whenever they are needed.

Lastly, there are two other areas of vulnerability that I want to address today. The first is supply chain security for our IT systems. Now we could get IT functionality perfect and a robust defense of networks in place and still be at risk of compromise from counterfeit components as well as unknown design specifications within an approved component, particularly, also looking at things like zero-day exploits which we know our adversaries make extensive use of.

So the second is the vulnerability of our critical infrastructure to cyber attacks. DOD relies on these services but they are defended by other Federal agencies or departments, or not at all. So I mention this frequently because I want to make progress in the effort to close these gaps. And today is another opportunity to see where we are on this matter.

So with that, again, I want to welcome our witnesses here today. Before turning it over to you—back to you, Mr. Chairman, I just want to take this opportunity to congratulate General Alexander in particular. This is grandchild number 15 was born today. A grandson. And General, I just want to congratulate you and your family on the addition to your family.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 31.]

General ALEXANDER. It is probably more than——

Mr. LANGEVIN. Thank you. And congratulations again, General. And I yield back, Mr. Chairman.

Mr. THORNBERRY. And then what State was he born?

General ALEXANDER. Texas.

[Laughter.]

Mr. THORNBERRY. Thank you. I just want to get that on the record.

Mr. LANGEVIN. Point well taken.

Mr. THORNBERRY. And I appreciate the gentleman's comments. And just as an administrative note, I want to remind members that next week, we have our first quarterly cyber operations briefing which is similar to the counterterrorism quarterly updates that we have been receiving. This is a new provision in the Defense Authorization Act, and we will have that classified briefing next week.

Without objection, all of your statements will be made a part of the record. And we would appreciate your summarizing them. We again appreciate our witnesses, the Honorable Teresa "Teri" Takai, Chief Information Officer of the Department of Defense; the Honorable Elizabeth McGrath, Deputy Chief Management Officer at the Department of Defense; and General Keith Alexander, Commander of USCYBERCOM.

Thank you all for being here. Ms. Takai, you may summarize your statement.

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

Ms. TAKAI. Good afternoon, Mr. Chairman and distinguished members of the subcommittee. Thank you so much for giving us the opportunity to testify today on the importance of information technology to the transformation of the Department of Defense.

I am responsible for ensuring the Department has access to the information, the communication networks, and the decision support tools needed to successfully execute our warfighting and business support missions. The Department's IT investments support mission critical operations that must be delivered in both an office environment and the tactical edge.

Just to give you some perspective on the size and scope of what we cover, we operate in over 6,000 locations worldwide. And we support the unique needs and missions of three military departments and over 40 defense agencies and field activities, and our services are used by 3.7 million people.

Included in the overall IT budget are the Department's cybersecurity activities and efforts that are designed to ensure our information systems and networks are protected against the ever-increasing cyber threats the Department and the Nation face.

We are undertaking an ambitious effort to realign and restructure our ability to provide better access to information, improve our ability to defend and keep pace. This effort is the Joint Information Environment [JIE].

The Department is aligning its existing IT networks into a Joint Information Environment that will define how we are restructuring not only our networks but our computer centers, our computing networks and cyber defenses to provide a singular joint cybersecurity approach that is common across the classified, secret, and coalition networks. This is in contrast to today's networks in which each military department differs in its approach and design in cyber defense.

The ultimate beneficiary is the commander in the field. The consistent network in IT and security architecture will enable innovative information technologies that keep pace with today's fast-paced operational requirements.

Our standard security architecture will enable cyber operators at every level to see who is operating on our networks and what they are doing. This will enable a synchronized cyber response. And I am sure General Alexander will be speaking more to you about this in his words.

The consolidation of data centers, operations centers and help desks will enable timely and secure access to the information and services needed to accomplish their assigned missions, regardless of the location.

As we have refined the JIE concept, we have concluded that we can achieve all of the Department's cybersecurity goals but just as importantly, still have better joint warfighting decision support, better operational and acquisition agility, and also importantly, better efficiency. On cybersecurity we are focused on ensuring that the essential DOD missions are dependable and resilient in the face of cyber warfare. The first of the efforts that we will embark on as I have mentioned is JIE. The second effort is our deployment and use of cybersecurity identity credentials for all users of our secret network. We are currently deployed on our unclassified network and we will complete the classified network this year.

The next is continuous monitoring. This will allow us much faster detection and remediation of mission vulnerability across the millions of computers that are in our networks, give us a chain of command and accountability tool, and will give the Cyber Command better ability to set remediation priorities.

The fourth effort as was mentioned is our supply chain risk management. Globally sourced technology provides real benefits to the Department but it also provides the opportunity for potential adversaries to compromise our missions through subversion of the supply chain. The Department recently issued policy that makes permanent the Department's efforts to minimize the risk to DOD missions from this vulnerability.

And lastly is our successful voluntary cyber information-sharing efforts with the Defense Industrial Base. We have 78 participating companies which represent a majority of our acquisition spending in the Department.

We share classified and unclassified cyber threat information and companies that have been participating said that the program has significantly improved their cybersecurity efforts. We are also partnering with security service providers, for those companies that choose to use that service, they will have additional classified threat information.

I would like to conclude by mentioning a few other efforts that we are working on. We have a new focus on the development of secure communications for Presidential and senior leader comms [communications], nuclear command and control, and continuity of government. We are working with other Federal agencies to ensure that we have the ability to communicate at all times. We are also working to ensure that the Department's position, navigation and timing infrastructure is robust.

Next, my office recently issued the DOD commercial mobile device strategy and implementation plan which allows us to use commercial mobile devices in both a classified and unclassified environment.

And finally, spectrum has become increasingly important not only to the Department's mission but to consumers and the economy of the Nation. While fully committed to the President's 500 megahertz initiative, it is important that we balance the use of our finite radio spectrum to meet national security requirements as well.

Thank you so much for your interest in our efforts and I look forward to taking your questions.

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

Mr. THORNBERRY. Thank you, Ma'am.

Ms. McGrath.

STATEMENT OF HON. ELIZABETH A. MCGRATH, DEPUTY CHIEF MANAGEMENT OFFICER, U.S. DEPARTMENT OF DEFENSE

Ms. MCGRATH. Thank you, Mr. Chairman. Good afternoon. We really appreciate the opportunity to discuss with you the progress that we have made in the defense business operations. We feel they are critical enablers of our national security mission and our goal is to ensure we have effective, agile and innovative business operations that support and enable our warfighters.

This work spans every organization in all functional areas. Our goals are to optimize business processes and identify key outcome-based measures. Here, information technology is a key enabler. Over the past number of years, attention to this issue has steadily increased and Congress has been instrumental in shaping the governance framework and supporting processes the Department uses to oversee these efforts. And we thank you for that.

My written statement provides updates on our integrated business environment framework; therein you will see evidence of the maturation of our Business Enterprise Architecture and some of the recent successes and challenges in the implementations of our largest IT systems.

I will take a few moments to highlight a few of the points. First, Section 901 of the 2012 National Defense Authorization Act included significant changes to the Department's investment management process for defense business systems. We established a single Investment Review Board which we execute through a Defense Business Council which replaced five separate functionally based boards.

It also significantly expanded the scope of the systems to be reviewed by the board to include those in sustainment. Previously, it was simply modernization and development. This new investment process allows the Department for the first time to holistically manage the entire portfolio of business systems in a deliberate and organized manner.

This legislation is truly serving as a catalyst for dramatic improvements across the defense enterprise. We now have functional strategies that articulate goals, outcomes, expectations, standards, mandatory solution across business lines.

Military departments and defense agencies all must align with execution plans to these imperatives across their IT portfolio. As an example of the Investment Review Board's value, we identified ap-

proximately 10 percent of the systems reviewed as legacy systems that will be retired over the next 3 years. And we are using this process to both ensure architectural compliance and business process reengineering.

Second, I would like to highlight the ongoing work to improve the implementation of some of the Department's most visible defense business systems, our Enterprise Resource Planning systems or ERPs. The Department is committed to learning from its successes and failures as well as learning from the findings from the Government Accountability Office and the Inspector General.

In addition to a number of ongoing initiatives to improve specific aspects of our implementations, I have over the last 6 months undertaken a substantial effort to work with industry leaders to fully understand and define the leading root causes of program successes and failures across the dimension of cost, schedule and performance.

Our findings reinforce the need to focus the Department on quality upfront work extremely early in a program's life cycle to include ensuring clarity of requirements, quantifiable business cases. As a result of this work, I have directed a number of actions across the Department.

While we have certainly faced challenges, the Department is making steady progress in this area including having now successfully fielded a number of Enterprise Resource Planning systems.

In closing, the Department remains committed to improving the management and acquisition of IT systems as well as our overarching business environment. These issues receive significant management attention and are a key part of our enterprise strategy to build better business processes that will create lasting results for our men and women in uniform and the American taxpayer.

I look forward to your questions.

[The prepared statement of Ms. McGrath can be found in the Appendix on page 54.]

Mr. THORNBERRY. Thank you.

General Alexander.

STATEMENT OF GEN KEITH B. ALEXANDER, USA, COMMANDER, UNITED STATES CYBER COMMAND

General ALEXANDER. Chairman, Ranking Member, I would read my statement but you know I can't read so I am just going to give you the highlights from that. And I know both Ms. Takai and Ms. McGrath can read really well. Perhaps you should read my part.

What I want to hit is a few things that I think it is important for the committee to know. First, you all know we have great people. We are getting great people both in our staff and the service components that have—that are building the teams that we need. And issues come up with sequester especially for the civilian folks; having to furlough those people that we are bringing in sends a wrong message.

Further, the continuing resolution compounds our ability to actually conduct the training missions that we need to bring these teams on board. We talked a great deal about the threat. You know what is going on in Wall Street, what has happened over the last

6 months. What happened in Saudi Arabia with Saudi Aramco, the threat is real and growing.

From our perspective, we need to be prepared for attacks against our Nation in cyberspace. In order to do this, we do it as a team. And that team includes DHS, Department of Homeland Security, FBI [Federal Bureau of Investigation] and, of course, DOD.

DHS has the resilience and recovery just like it would in a kinetic operation. And it is the public interface for our industry. FBI would lead investigations, look at who is doing this inside the United States; they are the domestic handler. And DOD has responsibility to defend our Nation from an attack, to support the combatant commands and their operations in planning, defend the DOD networks and other networks as authorized.

We have created roles and responsibilities between Secretary Napolitano, myself and Director Bob Mueller, we all agree on that, it has gone to the White House. I think that helps lay out the plan for how we can work with you in establishing legislation for the future. And I can talk to legislation and questions if that comes up.

When is civil liberties and privacy upfront here? We know how important that is. We can protect civil liberties and privacy in our networks. This isn't one or the other, it is both. And I think we can do both. And to understand that, I think we need to get into technical details. I won't do that here, but you know we have the capacity to do that.

And I just encourage you to look at the facts in this as we go forward. Five things that we are looking at from my perspective in setting up Cyber Command and the teams that we have. First and most important are people, building and training a ready workforce. The second thing, command and control and doctrine, we are establishing that and how we work with the combatant commands that I can answer more, Congressman Langevin, to your question later on about how we work with the combatant commands. Situational awareness—how do you see what is going on in cyberspace and how do you react to it. A defensible architecture, I think this is absolutely vital, especially for the Defense Department. Today, we have 15,000 enclaves. It is very difficult to defend and get situational awareness around that. We need to go the Joint Information Environment, something that we work very closely with Ms. Takai and her folks. And finally the authorities, policies and standing rules of engagement. Those are vital for the future and we need to work with you to get those right.

That is a quick summary of my 26-page written—and so, Mr. Chairman, I turn it back to you.

[The prepared statement of General Alexander can be found in the Appendix on page 62.]

Mr. THORNBERRY. Thank you. I think that may be a record on shortness of your testimony.

Let me just start by asking about a couple of things. General Alexander, I think the statements you just made that there is a role for the military, especially Cyber Command, to defend the country in cyberspace. I think that is a step beyond where we have been in previous years' hearings.

Can you tell us a little bit more about how that—where we are in that discussion? Exactly what should we expect the military to

defend us against and what sort of circumstances? And then what are the sort of circumstances that industries or us as individuals are required to defend ourselves?

General ALEXANDER. So there is two parts to this, to your question. And I will give it to you as accurately as I can from my perspective and then show you where the range of options that the administration and the Defense Department have to look at.

First, I think it is reasonable that we the American people know that when our Nation is under attack, whether it is physical attack or cyber attack, that the Defense Department will do its part to defend the country.

It is not going to just defend itself. Our job is to defend the country. And the focus would be, obviously, on critical infrastructure just as it would in kinetic and other things. The issue becomes when does an exploit become an attack and when does an attack become something that we respond to?

Those are policy decisions and the red lines that goes to those would be policy decisions. Our job would be to set up the options that the President and the Secretary could do to stop that. And as you may recall, both the former President and the current President have both said that they would keep the options open in this area.

I mean, I think that is reasonable, from using State Department to demarche all the way over to kinetic options or cyber. So they have that whole range. What we are building is the cyber options that would fit that tool kit for the administration and policymakers to determine exactly what to do.

As an example, it is reasonable to expect that we would have the ability to stop a distributed denial of service attack, and so creating the tools and capabilities of that, which would get into the classified area, you would expect that we would actually go and work with our teams to do that. And those are the kinds of things that we do. So how do we defend the country in that? What kinds of capabilities that we need? We have laid that out in great detail. And I think the training on that is superb.

Mr. THORNBERRY. Just to make an editorial comment. I appreciate your point that the authorities, policies, rules of engagement are key to deciding how to use the tools that your folks have evolved. My opinion is that the more the administration consults with Congress, the more we can make these decisions out in the open, the better result we will have and in addition, the more you will have the support of the American people.

The more that is kept secret with some White House meeting or White House paper that is hard to access to, the more suspicions there will be about what the government is really doing. So I know that is kind of a different realm from yours but I think the circumstances under which the government will act and how it will act and who will act are important to be as public and transparent as we possibly can.

Finally, let me ask, Ms. Takai, I have got this Defense Science Board study that came out in January that basically concludes, we cannot be confident that our critical information technology systems will work under attack from a sophisticated actor.

I mean, I am sure you have seen it. Can you just make a comment about whether you think this Defense Science Board study got it right about our vulnerabilities?

Ms. TAKAI. Well, I think, first of all, any independent report like that is useful because it does give us an independent view of a way of looking at our vulnerabilities. The report is a year old at this point in time and it really is—it does precede several of the actions that General Alexander has taken in terms of looking to remediate.

It also does not consider some of the actions that we have been taking to change our cyber defense approach from looking at how we protect the perimeter and how we just protect networks to actually how we look at it from a mission perspective.

So what we have done is ahead of actually the Defense Science Board report coming out, those are the same areas that we have been looking at. Those are the same areas that we are looking for remediation actions and some of the things that I described in my testimony are really a step toward actually moving forward to address some of those issues.

Now, the challenge is you are never 100 percent. And so, I think the point around, really, looking at it from a mission perspective is important because we need to be sure that we are prioritizing from the standpoint of where we put our resources, looking at it from the most critical areas and making sure they are secure.

Mr. THORNBERRY. If your folks look at this and think it appropriate, I would appreciate in a written answer some more updates as to how far you think we have come in addressing the shortfalls that they identified here.

Ms. TAKAI. Yes, sir. Absolutely. General Alexander and I are actually working on that document, so we would be happy as we get that developed to provide that to the committee.

[The information referred to can be found in the Appendix beginning on page 77.]

Mr. THORNBERRY. Thank you.

Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. Again, thank you to our witnesses. General Alexander, I would just start with you, if I could. More of a follow-on on to the chairman's question. Can you speak to the role of CYBERCOM as defender of last resort in the event upon civilian—in the event of an attack on civilian critical infrastructure?

As we know, these attacks move at network speed. And what I want to know is what the, you know, the processes that are put in place in terms of establishing rules of the road so that you know how and when you can respond—if there is an attack on critical infrastructure and CYBERCOM has to step in as the defender of last resort?

General ALEXANDER. So we are working with the Defense Department, the White House, and the interagency to set up those standing rules of engagement, put forward what I will call the way in which we would actually execute some of these.

Right now, those decisions would rest with the President, the Secretary. And they would tell us to execute. I think as we go down the road, we are going to have to look at what are the things that

you would automatically do, think of this as the missile defense, but missiles in real time.

And I think that is an education and learning process that changes fundamentally the way that we have defended the Nation from a kinetic perspective to how we are going to have to defend the Nation in a cyber perspective.

So there is a lot to learn there. Most important on that, one is the team that I talked about. But two is the partnership with industry. And that is where the legislation is going to be important.

We cannot see attacks going against Wall Street today. Somebody has to tell us, and if we are going to be able to react to it in time to have favorable results, we need to know that at network speed so that we can react at network speed. So those types of information-sharing and the liability of protection that goes with them is key to this. The other part, you know, you could put under building up standards and helping people get to this, the executive order takes a great step in that direction.

I think getting incentives would really help. So I think there is a partnership here, one within the administration for how we set this up and the rules of engagement, I take the chairman's comments that you put about working together in a transparent way. And the second part is we have got to have that same discussion with industry.

Mr. LANGEVIN. And let me use this as an opportunity to talk about the information-sharing, and give you an opportunity to talk about the, you know, the concerns that people have in terms of information that would be shared with the government.

I understand—you and I understand that we are not actually looking at information that would be shared, it is more the bits and bytes, the ones and zeros, the attack signatures that we would be looking for.

But I would like to again give you the opportunity for the public to reassure them of what this is, what information would be shared.

General ALEXANDER. Thank you, Congressman, because I do think this a key point.

The issue would be if somebody were throwing an attack at Wall Street, as an example, what we would want to know is the fact of the attack and the type of attack. We don't need to read people's email or see their communications to get that information.

The Internet service providers would actually see that. So we could tell them the types of attacks, the types of exploits and those things that the government needs to know. That includes DHS, FBI, NSA [National Security Agency] and the Defense Department, all together need to know that.

What we are talking about is, for example, I use the car going up the New Jersey Turnpike on its way to Rhode Island and it would go through an E-ZPass lane—well, in E-ZPass what happens is the car is scanned. You don't read what is inside the car. You just get the metadata.

In a similar way, if a packet were going forward, what the Internet service providers need to tell us is there was a packet, we saw bad software, malicious software in that packet, of the type you

were looking for. We stopped that packet. It was coming from this IP [Internet protocol] address, going to this IP address.

And it would be up to FBI if it was domestic to work with the courts to do that or to Cyber Command if it were coming from outside the United States. And so, the bottom line, there is a way to do this that ensures civil liberties and privacy and does ensure the protection of the country.

And I think we ought to work towards that and help educate the American people on what we are trying to do here.

Mr. LANGEVIN. I agree and I appreciate you getting that out there.

General, if I could, I would also turn our discussion to the new mission teams that are forming within your command. In testimony before the Senate Armed Services Committee on Tuesday, you noted the creation of 13 teams within—with an offensive focus. Can you lay out for us what authority these teams would be operating under and how will they interface with their Intelligence Community colleagues?

General ALEXANDER. Sure, Congressman. The key is we organize the teams into groups. So the teams that you are referencing, those 13 are what I will call the National Mission teams, that would have the mission to counter an adversary who is attacking our country.

They are the counter-cyber force. I call that offensive because their job is to stop—like a missile coming into the country, their job would be to stop that and provide options for the White House and the President on what more to do.

So they are the folks that would counter any cyber adversary. We also are creating teams to support combatant commanders and their missions and operations, and then we are building teams to operate and defend our networks within DOD and work with DHS and FBI as required.

So those are the three sets of teams and the three general missions that they have. And then, we have supporting them, what we call direct support teams that provide the analytic support that we would need for that.

All of this is integrated and works seamlessly with the Intelligence Community and with FBI to ensure we don't have duplication of effort and we are not all operating on the same place in cyberspace so that that is deconflicted.

Mr. LANGEVIN. My time is expired. I will have more questions for the witnesses in round two. I yield back.

Mr. THORNBERRY. I thank the gentleman. And I think it is helpful that explanation of what offensive means in this context because there is a variety of definitions that people use for that.

Dr. Heck.

Dr. HECK. Thank you, Mr. Chairman. I thank all of you for being here.

General Alexander, there have been some discussions about the roles of Cyber Command and protecting domestic critical infrastructure. How would that role differ if the attack was coming from OCONUS [outside the contiguous United States] versus CONUS [contiguous United States] and do you have the Title 10 authorities

necessary to respond to a domestic attack in real time since you are really the only entity that can defend in real time.

General ALEXANDER. Congressman, thanks, because I think for clarity, from my perspective, the domestic actor would be the FBI. And the FBI, we share our tools with the FBI.

They would work through the courts to have the authority to do what they need to do in domestic space to withstand an attack. We have worked very closely together.

Director Mueller and his teams are absolutely superb to work with. And we have come up with a way that he would do inside, we would do outside. Now, there may be points in time where you have different—you know, significant attacks where we need to change parts of that.

But the key thing is to have him do inside the country. We can support back and forth and do this at network speed. So we are practicing that. I think that is something that we can do.

He would work with the courts as appropriate to do his portion of the mission. Outside the country, that is where we would operate.

Dr. HECK. So you would be comfortable if there was a Saudi Aramco kind of attack that originated from within the United States at U.S. infrastructure, that the FBI would be able to respond and thwart that attack in real time?

General ALEXANDER. Assuming that we could see it because that kind of an attack is a whole different issue. And on that, where we would really depend is on working with the Internet service providers. They would stop that packet initially by some signature that we gave them.

And so, that is something that would go to a domain controller that we could stop. I think that is a different set of tactics that you would use versus the distributed denial of service attack where you are trying to take out the bots and the command and control infrastructure.

Dr. HECK. Okay. And then, how is the IC [Intelligence Community] supporting the cyber intelligence needs of DOD? I mean, beyond NSA, what IC organizations are the primary intelligence providers for CYBERCOM?

General ALEXANDER. Well, there are several, of course, the Central Intelligence Agency [CIA], the Defense Intelligence Agency [DIA] and NGA, the National Geospatial Agency. Tish Long and her folks have done a superb job, too.

It is kind of interesting. You say, "Well, what can you see from imagery?" But there are some great things that you can do by bringing the actual physical infrastructure and overlaying the cyber infrastructure—so all those work.

And within the military, DIA has, within our J2, people, at Cyber Command that work at—and of course, NSA has a great foundation of folks that really provide the best support that we have across that technical layer.

Dr. HECK. Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank you.

Mr. Kilmer.

Mr. KILMER. Thank you, Mr. Chairman.

I am particularly interested in workforce issues and how we prepare the workforce to meet the needs within the cyberspace. And I have a number of questions in that regard.

And I guess, Ms. Takai, I will start with you. As CIO [Chief Information Officer] you oversee the Information Technology Exchange Program that is set to expire on September the 30th, which seems like a good opportunity to leverage talent that is already in the workforce to bring industry and the Federal Government together, to knowledge share and learn best practices in cybersecurity.

I was hoping you would give a little update on that program's success and then I have a few specific questions therein. Do you feel like enough private companies know about the program and have been able to take part? Can you speak to the advantages of extending and/or expanding the program?

Have there been any problems with any aspects of the program that you think, if we looked at continuing it, should be addressed? And then, finally, I know to be eligible, an employee must be a GS–11 or the equivalent or above. Do you think that is an appropriate level or would you think there would a value in adding additional—involving additional workers in the mix?

Ms. TAKAI. Well, let me see if I can take all those questions in turn.

First of all, I think, we probably do need to expand our communications on that program. The program has been, I think, a great opportunity for us to bring industry technology experts into DOD and likewise, be able to look at where DOD employees can go out into industry to get experience.

But to date, we really do need to think about how we expand the program and from a communication perspective. However, I think it is important to note that right now, we have a key individual who has just recently joined my department from Cisco.

He is a very skilled, highly capable architect and one that is always difficult to grow. That kind of technical knowledge is something that just takes time. And so, the ability to bring that individual in and have them take a look at the work we are doing on the Joint Information Environment has really been valuable.

So we are really seeing the benefit of the program and therefore it is very important to us to continue the program. I think in terms of some of the challenges that we have had in terms of moving the program forward, it has really been understanding how to get the companies to understand the security requirements and for us to be able to get them in through our fairly long security process.

And I think some of that is just a part of it. But I think also we need to be in a position where we can better educate the companies on the kinds of security requirements that we are going to be asking about. And so, we are looking very much to take the lessons learned from the program, to be able to expand it. I think from a level perspective, I think starting at the GS–15s is sort of the—you know, the first level is actually a good place because it does give us the opportunity to go from the GS–11 level up through various levels, you know, into actually an SES [Senior Executive Service] level, which is the more highly skilled folks.

So I think starting there is a good place and the program does give us the flexibility then to bring people in at different levels. So we are very excited about the program. As I say, we appreciate the industry participation we have had so far and would very much like to continue the program past the sunset date in September.

Mr. KILMER. Thank you. Maybe just in follow-up, I would just like to ask more generally what you feel collectively we can do as Members of Congress to help you recruit an adequate number of workers in the cybersecurity realm?

Ms. MCGRATH. So I can say from a—again, I am more in the business space within the Department and it is always challenging to find skill sets even with the Enterprise Resource Planning and the more modern technological capability.

So we are buying commercial-off-the-shelf. It is really educating the workforce to get there. The Congress has passed legislation to enable us to hire highly qualified experts. I feel the Department has not leveraged the opportunity that we have so far, or to date, as much as we could have, really bringing folks in for a term.

It can be 1 to 5 years to work on some of these really sort of hard problems that we have, to ensure that our outcomes are what we need. But we do have actually a very good model in the SECDEF [Secretary of Defense] Corporate Fellows Program where we take our military and send them out to industry for a year at some of the, I would say, best and brightest companies like Cisco and Caterpillar and Google and—so we are not leaving anybody out, but I couldn't possibly mention them all.

Because they are already cleared, they have, I will say those kinds of requirements already met and it seems to be an easier transition from within the Department for our military externally, but I would wholeheartedly welcome, you know, anything we could do to advance the communication because I think it helps certainly in the business space with the activities we have under way.

Mr. THORNBERRY. Mr. Peters.

Mr. PETERS. Thank you, Mr. Chairman.

Just maybe a follow-up on that. I think, General, it was you who may have told us a few weeks ago about some of the difficulties you were having recruiting talented individuals in light of the budget uncertainty that we had.

That perhaps, people are coming to you and saying—I heard this at one testimony I think it was you—saying, "Gee, you know we can't really depend on this for a career if we don't think that Congress is behind it."

Last week, we took an action to relieve some of the pressure, perhaps, on the military side at the House level and that is working its way through Congress. But, do you want to update us, just to follow on Mr. Kilmer's question, how is the uncertainty around the budget or how is the budgeting continuing to affect your ability to recruit the kind of people we need to be our warriors?

General ALEXANDER. So, you have hit it right on the head, Congressman, that what we are getting from some of our people especially those who come from industry, they already take a pay cut coming to the government. And they do this because they are patriots.

The issue is they have taken a pay cut and now we are saying, "Well, you might get a pay cut again and this pay cut will be furlough and we are not sure how that is going to go, or where that is going to be."

That uncertainty is something that truly complicates their willingness to stay with us. And we don't—we should not do this to them. You know, we are trying to get the great people into cyber. These are technically qualified people.

You go out to Google, they are looking for people today. You know, I sat down with the Google HR [human relations] folks. They said, "Look, we are paying, you know, probably twice as much as you are paying folks" and they are having trouble getting them.

We get them because they want to do something good for the Nation. So as a consequence, I do think we have to, one, give them the certainty. I would just say, two, they are our most valuable assets. You know, it is the people. That is the talent that we need and we need to let them know we care about them, all of us, and we need your support in that.

Mr. PETERS. Thank you.

Thank you, Mr. Chairman. I yield back.

Mr. THORNBERRY. Thank you.

Mrs. Davis.

Mrs. DAVIS. Thank you, Mr. Chairman.

And I would certainly appreciate that comment because sometimes we have a perception out there that somehow Federal workers are not necessary to make everything work in this country. And I think that we know that that isn't true on just about every level. And so, I appreciate your comments.

I wanted to ask about the electronic health records. I know that is not exactly on the agenda right now. But I wonder if I could do that because we know that recently it was announced that the Department of Defense was going to—no longer are we going to have parallel efforts, I think, in trying to create an interoperable system. And that the Department of Defense was going to try and work with the Veterans Administration [VA]. Can you talk a little bit about that and what is going on? We had had that strategy articulated that they were going to do that, and it is just not clear now, exactly, what we are going to do.

I know that the discussion was around trying to cut costs, that we were going to create this common system, but in light of the fact that we are not going to do that, how are we going to create this interoperable system that is going to work?

Ms. MCGRATH. So I would be happy to take that question.

The Department of Defense and Veterans Affairs have been working together over probably 10 years to enable greater sharing of information between the two organizations. So when our military members transition from defense to the VA, that all their information comes with them and we could get out of a more paper-based approach to medical treatment and history.

And I think we have made significant progress in terms of sharing the information over big, I'll just say, pipes of interfaces between the two organizations. Both DOD and VA were looking to modernize their legacy environment.

And so, back in March of 2011, then Secretary of Defense Gates and Secretary Shinseki of the VA decided to abandon, if you will, either legacy system—so in VA it is VistA [Veterans Health Information Systems and Technology Architecture] and DOD it is AHLTA [Armed Forces Health Longitudinal Technology Application]—and move together jointly for sort of a common system, if you will, although it would probably be a family of systems that enable this capability to happen.

And we moved out smartly and made sure that we were approaching the solution, if you will, with a common architecture, a common data standard which is really key toward interoperability.

VA has moved their systems into our DISA [Defense Information Systems Agency], so that we are collocating as much as possible common business practices.

Because if you don't have all these things, you are still, I will just say, the IT will only get you so far.

And so, the foundational aspects of all these things we agreed to in 2011.

What you have heard recently, is the, in December of 2012 the Interagency Program Office had completed an engineering-based or bottoms-up, if you will, lifecycle cost estimate which really put the approach, the affordability of the approach, in question.

So the question Secretary Panetta and Shinseki said to the teams was, is there a more economical way to still deliver an innovative electronic health record to our military members and veterans, but it is done in a less risky way.

So you reduce the risk, decrease the cost and maintain the schedule that we are on. And that is when the Departments decided to instead of build, if you will, the system piece by piece, to start from a core set of capabilities and build out from a core.

So the VA decided to go back to their legacy system, again, VistA. The DOD does not have, right now anyway, a desire to use its legacy system and want to ensure that we have explored all opportunities.

So when we are looking at what would our core capability—would it be the VA's VistA core, VistA as our core? Would we look at—would we have something commercial? The health space has gone, has made tremendous leaps in terms of modernization over years. We want to ensure that we are assessing the capabilities that commercial market brings.

And we are right now—we issued a request for information in February. We got all the answer, all the responses in. We are evaluating them through our Cost Assessment and Program Evaluation team has the lead for that and they will make a determination whether or not we will go with a COTS [commercial-off-the-shelf]-based solution or a government-based solution by the end of March.

Mrs. DAVIS. Is it fair to say that we have kind of abandoned, though, the joint strategy?

Ms. MCGRATH. I think the joint strategy still exists from a data interoperability and integration. If I talk about a military member's health record, I am populating that record from data from different sources.

The change in the strategy is really the underlying IT system. We still want to do as much joint as we can from the various appli-

cations like immunization, lab, and all the other health-related stuff.

And I think that the architecture, again all the handshakes that we made in the beginning in terms of architecture data, those are all still absolutely at the forefront.

So there has been certainly a change with the approach to the underlying IT. But there has been no change to our——

Mrs. DAVIS. I guess what would be helpful to know about that is how is that going to affect the service member. And if they are—it sounds like you are looking at a new acquisition strategy perhaps. And I think we would certainly be concerned about costs involved and kind of, what have we lost I guess, in that time that we were working on all that.

So I just wonder maybe we can follow up with those discussions. But I appreciate it because I wanted to just take this opportunity to try and understand better what has happened and how we can move forward.

Ms. MCGRATH. Yes, ma'am, I would be happy to——

Mrs. DAVIS. We have spent a lot of time on that.

Ms. MCGRATH. We have and I would just say that all the infrastructure, the very foundational things that we have been working on since the agreement in 2011, all will be carried forward. And so, we are not, I will just say, scrapping anything from that perspective; we continue to use those foundational pieces because they are key irrespective of the applications that will ride on top of that infrastructure.

But I would be happy to give you more detail.

Mrs. DAVIS. Thank you. Thank you, Mr. Chairman.

Mr. THORNBERRY. I appreciate the gentlelady asking about that because I remember very well the hearing we had in the full committee with Secretary Panetta and Secretary Shinseki. And this was the key thing they trumpeted. Never before would we have this kind of cooperation between the VA and the Pentagon with one health record that would follow a service member from the day he enlisted all the way through.

And it is discouraging that under the best case scenario it is going to be significantly delayed to have that available as you all work through these various options. I don't understand or underestimate the technical difficulty in doing so.

I don't know. It is just frustrating I guess when this was trumpeted as such an achievement; that at least, there is a change in strategy.

Ms. McGrath, I am really not trying to pick on you but let me ask you about one other situation that maybe hadn't turned out so well.

The Air Force's Expeditionary Combat Support System [ECSS], what happened with that? And what have we learned from it?

Ms. MCGRATH. I would like to say—and I will very quickly move to the ECSS question.

But the two things on the electronic health record. One is the underlying system piece, and sort of the modernization.

What we are also focused on is accelerating data interoperability. We have standard data in the Defense Department across the entire organization. Because of the mobility of our military members,

the information must be wherever the military member is—that is theater, East Coast, West Coast, does not matter.

The VA—we are mapping the DOD health data dictionary to the VA data so that by the end of this year we will be using standard data between the two organizations and we will be able to populate a military record, an integrated electronic health record, with DOD and VA information.

And so I don't want to—I understand the concerns. I have been——

Mr. THORNBERRY. That is helpful, I appreciate you clarifying that.

Ms. MCGRATH. And so, we do. We are moving very smartly forward.

With regard to the Air Force logistics transformation program, true, not as positive a story. It was a story that began in the 2005 timeframe, and it was laden with I will just call them issues. We had a couple of protests along the way I think that added at least a year-plus to the program. We restructured it in 2009. They didn't meet a 5-year initial operational capability in the 2010 timeframe. So then we put I will just say stronger fiscal controls on the program to make sure that we identified success criteria both from a government perspective and a vendor performance perspective.

We also restructured the contract to be more outcome-oriented. And frankly, the program overall was not delivering. And, therefore, we cancelled it in the December timeframe of last year.

We have this in terms of this program that has provided many lessons learned as well as some of the other programs, both—some successful—we still learn from these programs and some not, in the area of size and scale this clearly was one of those programs that was way too big.

We need to chunk these IT systems, if you will, into smaller capability sets. And so, we are delivering and then adding as opposed to trying to deliver the whole thing at once.

Buy in leadership skill sets. And we talked a little bit about cyber skills and I mentioned the skill sets. Data, data quality is huge. For any of these IT programs, you are really trying to take really old data from old legacy systems, bring them into the new modern, much more tightly controlled environment. We have learned a ton with regard to data.

The infrastructure also can't be understated. The work that Ms. Takai is doing with the Joint Information Environment so that we have a much more holistic perspective on the network. How it runs, it is optimized. We find in every program I will just call it too much infrastructure, so it adds to latency and all of these kinds of issues. We have captured all of these, if you will, lessons learned along with some standardization of leading indicators across programs; we weren't managing and monitoring them in a similar way. And we have made those changes so that the program office, us, and us together, can look at really the health of each one of these programs as they move throughout the life cycle.

Mr. THORNBERRY. Well, to state the obvious I realize, but under the best case scenario we are going to have tight defense budgets as far as the eye can see. And a large amount of money goes to these various IT programs.

And obviously we have the same interest that you do, I know, into making sure that the money we spend is spent well and you get something for it.

It is particularly—I mean I appreciate the lessons learned, which are important absolutely. But it is frustrating also to spend money and then not have a system that works at the end of the day.

Hopefully, the lessons will improve others but it is something we are going to have to continue to get better about, no doubt.

Ms. MCGRATH. Excuse me, sir, may I add just very quickly?

Mr. THORNBERRY. Of course.

Ms. MCGRATH. Because I mean we do share both the desire to get it better and the frustration when it doesn't. And I am constantly looking for ways in how you apply the lessons learned from program A to program B or whatever the next one is.

But I would also say that I don't want to lose sight of some of the capability that has been delivered.

And the only data point that I will give you is that in 2009—and when we looked at the amount of money being spent on really we have about 14 of these major business programs. We were highly in a developmental stage.

The number of users in these main ERP [Enterprise Resource Planning] programs was about 27,000. Today, those same programs, we have 195,000 users. So we have delivered capability without going through the—I will just say the [word unclear] we tend to talk about, those that are sort of really big, expensive and not go so well. But there has been progress made in terms of delivering supply chain capability, financial capability, and also contracting. And I just don't want to lose that—and I appreciate you allowing me to share that.

Mr. THORNBERRY. Yes, ma'am. I appreciate it.

Kind of continuing on a theme of trying to spend smarter or at least exploring ways, Ms. Takai, the Defense Business Board made recommendations about satellite communications [SATCOM] and recommended that we could make some capital leases in multiple increments of up to 10 years. It has also been suggested that we could lease these satellite services for more than 1 year at a time which is what we have been doing and probably the most expensive way to do it.

Can you comment on that suggestion? And is that not something the Department should look at as a way of saving money for the commercial satellite services that we, that the Department depends so much on?

Ms. TAKAI. Yes, sir. We have seen the Defense Business Board recommendations and we do believe that there is benefit in looking at the cost recovery model that we are using for commercial SATCOM. And it is a requirement that we actually look at that over a multi-year period because of the nature of the industry.

So one of the things that we are doing is to actually put together a cost recovery model that takes into account a multi-year acquisition, to look at what is the best approach so that we can guide programs going forward.

We are implementing a converged SATCOM gateway architecture that will help to standardize more on the way that we are buying commercial SATCOM and actually our own SATCOM. We

are looking at a plan of action for our own nuclear voice conferencing integration and then looking at—we are actually conducting an analysis of alternative study as it relates to that.

One of the challenges for us is that when we look at commercial SATCOM, it is also important for us to look at the security of that commercial SATCOM. And in many cases, we are asking those commercial SATCOM providers to actually provide us capabilities that aren't necessarily the demand from the rest of their customers to the extent that we are looking at it.

So that requires some upfront investment for them, and if we are not able to actually commit to a multi-year capability, then we get into a couple of situations, neither of which is good. One of which is we would ask them to take that on and yet at the point in time we want to use it, we no longer have the funding in order to be able to do it.

On the other side, we fund it upfront and we aren't necessarily using the capability. That is why we need to look at a different way of the cost recovery model from a multi-year perspective in order to be able to manage the issue that was raised by the Defense Business Bureau.

Mr. THORNBERRY. Well, if there are additional authorities that you need to look at multi-year procurement of these services, please come and talk to us because I don't see if you are a satellite company how you can meet the Defense Department needs a year at a time particularly given what you just said about enhanced security requirements as part of that. I don't see how that can ever be done cost-efficiently without looking ahead several years.

General Alexander, I am going to take the other side of the argument now. This is a brochure from one of your two hats about commercial solutions for classified. And I guess it is inviting commercial companies to submit their products to see whether it could be used in a classified environment.

I mean—and I guess in a general way, is this a new emphasis on making more use of commercial hardware and software in a classified environment? And can we do that in a secure way? Again, thinking back to the Defense Science Board saying we got problems here.

General ALEXANDER. Chairman, I think we can. A couple of areas. If you think about encryption capabilities, going out and getting commercial encryption and making sure that it meets the standards, and we can set the standards based on different encryption levels. We can if we know the company and the way they actually create the capabilities, the tokens. And you can look at some of the DOD cards and stuff that we actually use. We can ensure that it is done right, then there is a great opportunity for us to work with industry.

I think this is going to become hugely important as we grow mobile devices that, you know, our spouses will use for banking, need to be secured at a comparable level to the way that we would need to do classified and sensitive operations.

So ensuring that the devices have that capability not only helps industry, it helps the government, and I think there are great ways to do it. We look at that in some of the encryption stuff we work with NATO [North Atlantic Treaty Organization] and elsewhere, so

I do think it is a great step forward, and industry does provide us some great capabilities.

Mr. THORNBERRY. Mr. Langevin.

Mr. LANGEVIN. So maybe on that line of commercial, let's talk a little bit about the cloud as where—we seem to be moving more and more toward the cloud. You know, articles that I have been reading recently have diminished my confidence in the security of the cloud, at least it has called it into question anyway.

There have been some high-profile thefts of information from that, in that realm. And yet I know that certainly is something that your operation, General, are looking at moving more into, more in that direction.

Let's talk about the security of the cloud. And if we do make a robust change in that direction, you know, what are we doing about guaranteeing security? What is your level of confidence in securing the cloud?

General ALEXANDER. So this has several dimensions to answer that question. I am going to try to hit each of those, and then if you want more information, we can come back.

First, when we talk about cloud security versus what we call legacy architectures, the problem that we have with legacy architectures is if you look at the Defense Department's 15,000 enclaves with administrators for each of those enclaves, the ability to patch those networks and set vulnerabilities is at the manual speed.

And the problem that that creates if you say that the time a vulnerability is publicly identified until it is done in the Department, it takes way too long because it is done to those 15,000 network parts.

We are using the host-based sensor systems to help speed that up but it is not where it needs to be. And your ability to actually see into those enclaves is very difficult. So the first thing that a cloud can give you is the ability to patch those systems almost in real time. You can reach out and patch that network there.

Now there are some issues that we have had with the cloud. One of the things that we saw is the cloud systems as we saw them did not have data element-level security tagging capabilities. So in the one that we created, Accumulo, we allowed it to have each element of data tagged and secured at that level, and only accessible at that level.

And there are some exceptional things that we can do in this area that I can go into more detail in another setting that gives you how I think this is more securable than legacy architectures. From our perspective, from our technical perspective, it is much better. It is not perfect. The issue is somebody who hacks into your networks over here, you don't know where they are but they have free—they are free to roam around once they are inside. You just don't know they are there.

As you may know, most companies that get hacked in the legacy system don't know about it for 6 to 9 months. I think we can go much further in the cloud and I think you will see that that will far outstrip legacy architectures in security. Unless you come up with an architecture that is completely independent, nobody else can get into.

But for what we need it for the Defense Department, we need mobile secure comms [communications]. And when you think about it, think about our ships, our aircraft and our mobile teams out there, they have to talk to something in the mobile environment. They are going to end up talking to the cloud. So we have to fix that cloud environment.

I will tell you that what Ms. Takai and her folks are doing with the Joint Staff J6 and our folks on the JIE is a huge step in that direction. It will address all of those types of issues and there is more. You know, I feel like the Ginsu knife guy—"wait, wait, wait, there is more"—because, you know, think about what you can do in a cloud that you can't do in a normal system, just to give you a couple of ideas.

You can jump your networks, you can jump your databases, like frequency-hopping, that makes your ability to hack into them very, very difficult; and each day down that can be encrypted with a different algorithm depending on the security levels of the people who need access to that data. That is a huge step forward. We are having tremendous success in that area. And I think you have seen some of the folks who are working on that.

I think you may talked to some of them, Dave Hurry and some of the others that are really good at that.

Mr. LANGEVIN. Well, thank you for the answer. That helps quite a bit. If I could, let me turn now to Ms. Takai. So obviously this is, you know, all of these great technologies that we have ultimately come down to the people.

How well they are trained, do they know the capabilities of the systems and so—I know you touched on this a little bit but can you speak further to us about how you are developing the pipeline of cyber and IT professionals in the Department and are there things that we can do better to support you? And I know you have talked on this a little bit, I would like to give you an opportunity to expand on this even further if you would.

Ms. TAKAI. Thank you very much. Well, first of all, let me just give you a synopsis of the actions that we are taking around growing the cyber workforce. The first steps are really around being able to support General Alexander and making sure that as we are growing the cyber capabilities, we are doing it to the requirements of what he feels he needs from the cyber workforce perspective.

So it is important that we recognize that the capabilities that we are growing are going to be operational capabilities and we are really focused on that partnership and making it happen. We are putting together that strategy today. The first grouping will be individuals that we have inside DOD and we will need to update our certifications, we are going to need to upgrade our capabilities.

And the other thing I think and General Alexander can speak to this even more. It isn't just necessarily technical people that are going to be on these teams. It is going to be a breadth of experience and it is going to really need several capabilities. Now, just to speak to the technical side of it, we are going to be bringing in and growing the resources from some of the technical people that we have today.

The plan is through the Joint Information Environment really as we begin to implement it, we will be able to free up individuals

who can then be trained with some of the technical background to be able to move into the cyber defense area much more heavily than they are today. So that is one—number one.

And then secondly is we are going to step up our recruiting and with that we are going to have to be more definitive around the career path for the civilians that we hire. Clearly, the military and General Alexander is addressing how the military will be moving folks through. But one of our challenges is we aren't going to be able to rotate people in and out of jobs in the same way, because the skill sets that are required here means we need to have a single career path for these individuals to continue to grow.

And that will be an area that we will want to come back and talk with you about because today the way that we do that career development doesn't necessarily allow us to keep people in a single path and move them up progressively, it tends to move them around from position to position. So, that is an area that we will be back to you.

The third area is that we are going to have to find a way to be able to recruit individuals at the more senior levels to be able to supplement. We are not going to be able to grow everybody from within. And that is an area where we are going to have to look at our existing programs to see what we can do from a competitive salary perspective.

We can get a lot of good people because the national mission is important, but at the same time we are going to have to look at what those sources of individuals would be and that would be as I say not only looking at our university systems and being able to grow them, but also what will it take to recruit some of them from the outside.

Mr. LANGEVIN. Thank you. Further, you know, to talk about this issue of integration, how are you planning to integrate our total force capability such as those resident in the National Guard cyber units into a comprehensive CYBERCOM approach, particularly with regard to command and control and authorities?

Ms. TAKAI. Let me start and then ask General Alexander to comment on this as well. We believe that the National Guard does provide a great opportunity to actually look at being able to look at other forces. So for instance, particularly in areas like Washington, particularly around Redmond, and in the areas of Silicon Valley, we know already that we have individuals that are in the National Guard that are highly capable.

The key thing I think is to make sure that as we utilize the National Guard, we are doing it in not only a uniform way but we are doing it in a way so that we have the advantage in two senses. One is that it is integrated with the entire cyber approach that General Alexander is going to speak to. But second of all, that as we are moving people through there and as we are actually utilizing them in different settings, that again they are going to be operating in the same way, they are going to be able to be integrated rather than them having sort of a separate approach to the way they are doing the training and not be able to call them in when they are needed.

But General Alexander, let me have you also talk to how they are going to fit within your teams.

General ALEXANDER. Congressman, I would add also the great teams in Rhode Island, Texas and Nevada, just to get all three of them out.

Mr. LANGEVIN. The 102nd in Rhode Island.

General ALEXANDER. And of course, I know Ms. Takai wanted me to mention those. We sat down with the National Guard a couple weeks ago. We have had our first Guard exercise last summer. We will have another one this summer. As Ms. Takai said, we are training everybody to the same standard. My comments to them is, look, your folks have to be trained and certified to the same standards as the Active Force.

Our focus would initially be on the cyber protection teams that they would create. And I think they will focus on regional teams. The 10 regions of the Guard, create those teams first, train them and operate them. See what their role and relationship would be working with us, DHS, FBI and NORTHCOM [Northern Command] defense support to civil authorities. There are some great things that we can do.

We will also create some offensive teams and some of the Guard units are already doing that. I talked to General Grass today on this topic. He, General Jacobi and I will meet next Tuesday and perhaps we are going to meet right now. That must be him calling in.

We will meet next Tuesday to actually lay out a transparent program so the service chiefs see what we are buying. We want to make sure that this is a program the service chiefs sign up to because parts of this are going to be in their budget and we want to make sure that everybody is transparent in what we are getting here.

So that is the process. There is a Cyber Guard exercise coming up. I think those are some of the things that you and some of the other members may be very interested in; you are welcome to attend parts of that.

Mr. LANGEVIN. Thank you. I am very impressed with the work of the National Guard and as you have mentioned we have the 102nd in Rhode Island that is actively working with various aspects of cyber, particularly with the 24th Air Force. I have had the ability to get down to the 24th Air Force in Texas and visit with General Vautrinot there. And I know that they are working very closely with our Rhode Island National Guard in that respect.

General, as always, we thank you for—and your team. Please pass on our appreciation to the extraordinary men and women under your command and also, Ms. Takai, at the Pentagon, for the work that they are doing, how dedicated they are, it is obviously very important. We want to do everything we can to support you and before I yield back I just want to thank the chairman for his partnership in this effort as well.

There are very few people in the Congress—not enough—that focus on this issue of cybersecurity and I know, Chairman Thornberry, how much you put a lot of time and effort into this issue and there is not another Member of the Congress that has worked as hard on this issue as you have, so thank you.

Mr. THORNBERRY. I appreciate it, Jim—obviously, the gentleman has been a leader in this for some time. Dr. Heck, do you have other questions?

I just had two more things I wanted to ask about. General Alexander, to the extent you can talk about it in open session, this subcommittee has been interested before on tactical use of cyber in military operations. And I noted that part of your teams, the teams you are creating in Cyber Command, are those teams—some teams to support combatant commanders.

And can you in this forum describe how that will work, to whom they will answer, how it will be decided what operations to carry out and whatnot, that sort of thing?

General ALEXANDER. Chairman, broadly speaking they are going to work at the strategic level, those combatant command [COCOM] mission teams will be directly focused on the COCOM requirements and answer to those requirements.

We will have a deconfliction process that that combatant commander and myself will work together to make sure that if somebody else is working in that space we deconflict it, and that is logical so that you don't have two people working in the same space.

That is different than the tactical service teams that we would create. So if you go into Iraq like in the past 10 years and look at what we did for our intelligence teams that support brigade combat teams, that was a huge success.

In the future, you can imagine that we will eventually grow, at the tactical level, cyber teams that are part of those intelligence teams or working together with them to provide local cyber effects. They would have to be trained to the same standard, deconflict through a theater and others, just as we do other areas. But I think it would provide that.

And then you can see that the Air Force and Navy would have tactical and operational level that would nest into what we are building at the combatant command level. So I think they will work as a team, think of that as a cryptologic architecture now for cyber going all the way down. And I think this provides us tremendous capability at the tactical edge.

Mr. THORNBERRY. I fully agree, it does. I guess, what I haven't quite got my mind around is how you deconflict what you think is a tactical operation when there really is not geography in cyberspace. And so the equities that—part of our—my concern has been that if you want to have a tactical cyber operation, you basically have to have a full complement of all the agencies in Washington to hash it all out. And that is not very time efficient for cyberspace and just how that would work on a practical basis. I think we got to work our way through it. It is just something that I have been interested in and we have worked on from time to time. Do you have one——

Ms. Takai, we could not have a hearing without me asking a question about spectrum, because it is such an important part of what goes on. I know there was a recommendation for sharing spectrum as a possible, I don't know solution, but as a possible step that could increase spectrum for anybody. Do you have any comments on that recommendation?

Ms. TAKAI. Yes, sir, and I was wondering whether we would get to the spectrum question or not, so here we are. We actually feel very strongly that it is important that we look at spectrum-sharing as a possibility.

I think the report that you are referring to is probably the President's PCAST [President's Council of Advisers on Science and Technology] report that suggested that we have to look at spectrum-sharing going forward. We are participating now in five different working groups that are being led by the NTIA [National Telecommunications and Information Administration] to look at different areas of spectrum-sharing.

And we actually have had success in spectrum-sharing. We have had an instance where we have been able to actually use and be able to share with a medical device, a medical alert device for some of the areas. So we do believe that there are opportunities.

But with that, spectrum-sharing has its challenges. It isn't a new concept; it is certainly just coming to light now because of the severe pressure on spectrum. There are several different ways to do it. One of them is geographic, where you look at exclusion zones.

The difficulty for us in certain bands, like the 1755 to 1850 band, is that the exclusion zones would actually be in the same areas that the commercial providers are interested in. So we have to look at that. The second thing is whether we could do it from a time standpoint.

But again in 1755 to 1850 which we use very heavily for training in CONUS, that becomes difficult because we can't predict where in fact we are going to be in the timeframe we are going to be using it.

So I think it is—there are great opportunities. I think we do need to explore and we are working and have signed some of the first ever MOUs [memorandums of understanding] with the some of the commercial companies to actually do some experimentation in certain geographic locations.

But I think it is a step beyond where we can, you know, necessarily say we can go to say that spectrum-sharing is going to solve the problem. It is really a combination of where do we have to vacate, where will we need comparable spectrum, and then where are the areas that we can share now and then going into the future.

Mr. THORNBERRY. Thank you. And thank you all again for your patience and for your brevity. We hit on a wide variety of topics today and that was very helpful. And as the gentleman from Rhode Island said, we appreciate each of you and the folks who work with you and what they do for the country.

With that the hearing stands adjourned.

[Whereupon, at 5:05 p.m., the subcommittee was adjourned.]

A P P E N D I X

MARCH 13, 2013

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 13, 2013

Opening Statement for Congressman James R. Langevin (D-RI)

Subcommittee on Intelligence, Emerging Threats and Capabilities will meet to receive testimony on Information Technology and Cyber Operations: Modernization and Policy Issues to Support the Future Force.

March 13, 2013

Thank you, Mr. Chairman, and thank you to our witnesses for appearing before the subcommittee today. This is an important hearing, as our national security is dependent on our information systems. Those networks are critical to all aspects of our defense, yet one only needs to look at recent news headlines to understand the unrelenting and sophisticated threats that we face in the cyber domain. We continue to see just how vulnerable such networks are in other sectors of our society, at a potential cost of billions lost to cybercrime, and we know our defense networks are at even greater risk. They must be fail-proof and secure.

We are still waiting for this year's budget, but I believe it is safe to say that IT represents a large piece – $33 billion last year. That is a significant figure, and we must be ever mindful of our responsibility to make the most effective use of taxpayers' investments in these capabilities. We are aware that the Department has experienced some challenges in acquiring certain IT systems and services in the past, so today I'd like to hear what steps we are taking to tackle those challenges in order to get the connectivity we need at a reasonable price.

DOD Cyber operations are quite literally a growth business. It is one of the rare portions of the DOD that will be growing indefinitely into the future, and there have been significant developments in just one year since our last posture hearing. We are starting to get answers to some questions about how and when the United States might conduct the full range of military cyber activities, and I'd like to discuss that today to the extent that this forum allows. I understand that Cyber Command is beginning to organize itself into mission teams, which is an exciting step, but the manpower cost is enormous and the education and training requirement significant. This is going to take a lot of work to get right. I would be greatly interested to hear our panelists' thoughts on how we refine the education, recruitment, retention, and training of the highly specialized personnel we need. I

would also like to hear how CYBERCOM is interfacing with combatant commanders to provide its unique capabilities wherever they are needed.

Lastly, there are two other areas of vulnerability that I want to address today. The first is supply chain security for our IT systems. We could get IT functionality perfect, and a robust defense of networks in place, and still be at risk of compromise from counterfeit components as well as unknown design specifications within approved components. The second is the vulnerability of our critical infrastructure to cyber-attacks. DOD relies on these services but they are defended by other federal agencies and departments. I mention this frequently, because I want to make progress in the effort to close these gaps, and today is another opportunity to see where we are on this matter.

STATEMENT BY

TERESA M. TAKAI
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

INTELLIGENCE, EMERGING THREATS AND CAPABILITIES

ON

DOD INFORMATION TECHNOLOGY AND CYBER OPERATIONS PROGRAMS

March 13, 2013

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), especially during these challenging budget times. I am Teri Takai, the Department's Chief Information Officer (CIO). My office is responsible for ensuring the Department has access to the information, the communication networks, and the decision support tools needed successfully execute our warfighting and business support missions. Our mission is to ensure that these capabilities can be depended upon in the face of threats by a capable adversary in all conditions from peace to war, and particularly in the face of cyber warfare by such an adversary. My focus in accomplishing these responsibilities is to ensure the effectiveness, reliability, security, and efficiency of DoD's IT capabilities for the warfighter, and ensure we are able to take advantage of future technology innovations to support the Department's missions.

I would like to give you an overview of some of the key IT and cybersecurity initiatives and efforts currently underway in the Department and what we are doing to ensure our warfighters have the capabilities they need when going into harm's way. I will start with a broad overview of the Department's IT landscape, and then describe the Joint Information Environment (JIE), which is our effort to restructure much of the underlying network, computing, and cyber security of the department so as to make us more agile in deploying new decision support capabilities, make us better able to mount cyber defense of our core Department missions, and to make us more efficient. I will also discuss the Department's cybersecurity efforts and describe some important initiatives specifically intended to better support our warfighters. Finally, I will discuss the cyber and IT workforce and our efforts to change the way information technology planning and budgeting is done in light of all of the above.

Overview of DoD's Information Environment

The Department's FY14 IT budget request is still being finalized, but will include funding for a broad range of information technology, including: desktop computers, tactical radios, identity management technology, commercial satellite communications, business systems, cybersecurity 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, and to 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. Included in the overall IT budget are the Department's cybersecurity activities and 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. These efforts continue to receive the highest-level attention and support of the Department.

The scale of the Department's networks illustrates 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. This totals 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 they 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.

Joint Information Environment and Joint Force 2020

Increasingly, mission success depends upon the ability of our military commanders and civilian leaders to act quickly and effectively based on the most accurate and timely data and information available. Recognizing that information is a strategic asset, DoD is undertaking an ambitious effort to re-align and restructure how our many IT networks are constructed, operated and defended in order to provide better access to information to the user, improve our ability to not only defend the networks and the data, but make it responsive to the constantly changing technological and operational factors. The challenge is amplified because our adversaries are

trying to use every opportunity to penetrate our critical infrastructure to capture, disrupt, or destroy our information and to do harm to our forces. Consequently, DoD is pursuing the alignment of existing vast IT networks into a Joint Information Environment (JIE). JIE will have federated networks that are built to common standards and configurations, and expanded use of shared IT infrastructure and enterprise services, which include Thin clients, everything over IP, email, and cloud services. The Services will continue to operate and maintain their portion of the JIE, as well as provide mission-unique capabilities while incorporating shared IT transport services and common applications.

The Joint Force faces a shrinking technological lead and growing vulnerability in a variety of systems, most notably in IT. We see increasing emphasis and resource expenditures by our adversaries focused on disrupting our command and control systems. Based on increasing threats in Cyber, decreasing budgets, and the explosion of new IT capabilities and solutions, the Department has engaged in a series of efforts to strengthen and deliver a more agile, secure information capability to enhance combat power and decision-making.

The Chairman of the Joint Chiefs of Staff recently issued "Joint Force 2020" as a vision for how the Joint Force of the future can effectively address security challenges through globally integrated operations. This will help increase the overall adaptability of the force to cope with uncertainty, complexity, and rapid change.

A primary enabler of this vision and strategy is the JIE. First and foremost, JIE will improve mission effectiveness. It is intended to enable and empower our military's decisive edge—our people—by providing warfighters and our mission partners a shared IT infrastructure consisting of federated networks with common configurations and management, with a common set of enterprise services, within a single security architecture.

The JIE will change the way we assemble, configure, and use new and legacy information technologies. It will consist of enterprise level network operations centers that will reduce the complexity and ambiguity of seeing and controlling the numerous networks within DOD; a set of core data centers – significantly reducing the current number of DoD data centers while ensuring the information is secured and available where needed; and standard, single security architecture that will reduce the number of organizationally owned firewalls, unique routing algorithms, and

inefficient routing of information that currently exists today. Together with the single, authoritative identity management and access control, emerging cloud capability, mobile computing devices and data-focused applications, and , common IT enterprise services, JIE will provide the information environment to flexibly create, store, disseminate, and access data, applications, and other computing services when and where needed. It will better protect the integrity of information from unauthorized access while increasing the ability to respond to security breaches across the system as a whole.

On both classified to unclassified domains, our employees, including warfighters, will have the ability to connect to information resources needed from any device, at any time, from anywhere in the world. Furthermore, as individuals move around the world, whether for operational deployment or in support of business operations, their movement within the information environment will be virtually seamless and allow them to immediately operate from any device.

In today's environment, the Combatant Commands (COCOMs) are provided with Military Service-centric IT networks and IT services operating on Service–unique domains. This Service-centric approach extends beyond networks to identity and access management processes, data centers, mission and business applications, commercial off-the-shelf (COTS) hardware and software, and IT procurement practices. The result is an IT infrastructure that does not effectively support the joint warfighting environment.

The ultimate beneficiary of JIE is the commander in the field, allowing for more innovative integration of information technologies, operations, and cyber security at a tempo more appropriate to today's fast-paced operational conditions. Specific benefits include:

- A standardized information and security architecture will improve how DoD operates and secures its networks on a global level. Users and systems will be able to trust their connection from end to end with the assurance that their activity will not be compromised.

- The JIE's standard security architecture will enable cyber operators at every level to see the status of their networks for operations and security and enable commonality in how cyber threats are countered. The Department will know who is operating on its networks and what they are doing, and be able to attribute their actions with a high degree of

confidence. This will minimize complexity for a synchronized cyber response, maximize operational efficiencies, and reduce risk.

- Consolidation of data centers, operations centers and help desks will enable users and systems to have timely and secure access to the data and services needed to accomplish their assigned missions, regardless of their location.

- A consistent DoD-wide IT architecture supports effective fielding of Department capabilities in support of information sharing, as well as sustainment and integration of legacy systems.

There will be investment required to effect the transition from the Department's as-is environment to the desired to-be state. The Department will utilize the Services existing programs, initiatives, and technical refresh to deploy or migrate to JIE standards utilizing specific implementation guidance.

Data Center Consolidation

An important aspect within JIE is the active consolidation of the Department's numerous data centers. These efforts are consistent with and support the Federal Data Center Consolidation Initiative (FDCCI) being led by the Federal CIO

The Department recently compiled a global inventory of its data centers, and is establishing four classes of data centers to assist in the development and execution of our data center consolidation strategy. These four types of data centers are:

- Core Data Center (CDC) – delivers enterprise services and provides primary migration point for systems and applications; these are our most important data centers, strategically located to provide speed of access to global information requirements;
- Installation Processing Node (IPN) – provides local services to DoD installations and hosting systems not suited for CDCs, these will be located at the installation level, and will consolidate the duplicative data centers at the installations;

- Special Purpose Processing Node (SPPN) – provides compute and storage for fixed infrastructure or facilities, such as test ranges, labs, medical diagnostic equipment, and machine shops.
- Tactical/Mobile Processing Node (TPN) – provides support to the deployed warfighter at the tactical edge; these unique "data centers" directly support the warfighter in a disadvantaged or tactical environment, but connect back into the Generating Force information sources and core data centers.

The DoD Core Data Center Reference Architecture was published in October 2012 and provides the foundation for the DoD's data center consolidation efforts as well as supports the emerging Department's Cloud Computing capability, which will be "tied" to data centers.

Significant progress is being made in data center consolidation, and plans are in place close nearly 50% of all DoD data centers within the Future Years Defense Plan with the remaining data centers transforming and conforming to standards to achieve the JIE.

DoD Mobile Device Strategy

Last year, when I testified before this Subcommittee, I described several mobile device pilot efforts the Department had underway. Since that time, my office has approved broader deployment of smart phones and tablet computing for unclassified use within the Department. the DoD Mobile Device Strategy was published on June 8, 2012, which identified IT goals and objectives to capitalize on the full potential of mobile devices in the Department. The strategy focused on improving three areas critical to mobility: the networking infrastructure to support wireless devices, mobile devices, and mobile applications, and a framework will ensure the Department's use of commercial mobile devices is reliable, secure, and flexible enough to keep up with fast-changing technology.

As follow-on to the Strategy, my office recently (on February 15, 2013) issued the DoD Commercial Mobile Device Implementation Plan. The implementation plan establishes a framework to equip the Department's 600,000 mobile-device users with secure classified and protected unclassified mobile solutions that leverage commercial off-the-shelf products, encourage the development and use of mobile applications to improve functionality, decrease

costs, and enable increased personal productivity. The plan orchestrates a series of operational pilots from across the DoD components that will incorporate lessons learned, ensure interoperability, refine technical requirements, influence commercial standards, and create operational efficiencies for DoD mobile users. The DoD Mobile Device Strategy and Implementation Plan aim to align the various mobile devices, pilots and initiatives across DoD under a common security and cost framework that aligns with efforts in the JIE. This is not simply about embracing the newest technology – it is about keeping the Department's workforce relevant in an era when information accessibility and cybersecurity play a critical role in mission success.

Key partners in these efforts are the Defense Information Systems Agency (DISA) and the National Security Agency (NSA), who working together with industry, have developed security configuration baselines for several of the major smart phone technologies and are working on more. The Services are also actively involved in these efforts and will be responsible for helping develop mobility applications.

Enterprise Services

As noted above, enterprise services are those global applications that can be used by many, if not all users within DoD. They are a key element of achieving more effective operations and improved security across the Department. An example of what the Department is doing in this area is Defense Enterprise Email, which is an enterprise messaging tool, built by consolidating existing disparate email servers into a global capable server and operated by DISA on a fee-for-service basis, which provides DoD with a common enterprise directory service and a consolidated email service.

The enterprise directory service is being incorporated by many organizations, and the Defense Enterprise Email is currently used by DISA, EUCOM, AFRICOM, USFK, Defense Manpower Data Center, Office of Naval Research, Navy Recruiting Command, the Joint Staff, and the US Army. As of March 2013, there are 976,000 enterprise email users on the Department's unclassified network and 21,000 users on the DoD Secret network, and continued adoption and consolidation to this capability is expected in the future.

In June 2012, my office completed a report to Congress stating that decisions to consolidate organizational email capabilities beyond the current user community, such as Navy, Marine Corps and Air Force, are being considered and will be validated using a business case analysis.

Cloud Computing

Cloud Computing is becoming a critical component of the JIE and the Department's IT modernization efforts and will enable users the access to data anywhere, anytime on any approved device. One key objective is to drive the delivery and adoption of a secure, dependable, resilient multi-provider enterprise cloud computing environment that will enhance mission effectiveness and improve IT efficiencies. Cloud services will enhance warfighter mobility by providing secure access to mission data and enterprise services regardless of where the user is located and what device he or she uses.

My office recently issued the DoD Cloud Computing Strategy to provide an approach to move the Department to an end state that is an agile, secure, and cost effective service environment that can rapidly respond to changing mission needs. There are two key components of the Department's cloud strategy. The first component is the establishment of a private enterprise cloud infrastructure that supports the full range of DoD activities in unclassified and classified environments. The second is the Department's adoption of commercial cloud services that can meet the Departments cybersecurity needs while providing capabilities that are at least as effective and efficient as those provided internally.

The DoD's Enterprise cloud infrastructure will provide shared technology capabilities for the consolidation of stovepiped services at installations and in core datacenters. It also will define connectivity standards for end-user devices, unmanned clients and other networks. This will enable the Department to develop and deliver new and more integrated enterprise information services that support our warfighters and business support operations, which will improve the effectiveness, security and reliability of those operations.

The DoD CIO continues to investigate new ways to leverage commercial cloud computing innovations and efficiencies to improve the Department. The nature of the Department's mission, and the risk to national security if DoD information were to be compromised, requires the careful evaluation of commercial cloud services, especially in areas of information assurance

(IA) and cybersecurity, continuity of operations, and resilience. To improve our cybersecurity posture with regards to commercial cloud computing, we are participating in the Federal Risk Authorization and Management Program (FedRAMP) and updating our own cybersecurity policies.

I have designated DISA as the DoD Enterprise Cloud Service Broker to facilitate and optimize access and use of commercial cloud services that can meet DoD's security and interoperability requirements, and ensure that new services are not duplicative of others within the Department while consolidating cloud service demand at an enterprise level. In addition, DISA, as the DoD broker, will leverage the FedRAMP standardized security authorization process, including the accepted minimum security baseline for low and moderate services, and ongoing continuous monitoring to ensure that appropriate security controls remain in place and are functioning properly.

Cybersecurity

Cybersecurity is one of the highest priorities of the Department and the Administration. The primary cybersecurity goal of my office is ensuring that essential DoD missions are dependable and resilient in the face of cyber warfare by a capable adversary. This is also a primary concern driving the other improvement efforts, particularly JIE. This focus on mission assurance, rather than on computer or system security, is one of the primary changes in the department's cybersecurity approach. In addition, another change is the focus in JIE of giving certain operational commanders more freedom to take operational cyber security risks. We do this by using "risk zones" in the design of the JIE computing and networks; these zones help keep the risks assumed by a particular mission from spilling over into other missions. This is also a significant change from today's DoD networks which impose more operational constraints on commanders. Other primary cybersecurity goals include improved safe sharing with whatever partners a mission requires, and a continued need to keep a secret. Through refinement of the JIE concept, including the JIE single security architecture, we have concluded that all of these cyber security goals can be achieved, and the Department will have better joint warfighting decision support, better operational and acquisition agility, and better efficiency.

Like other IT efforts, cybersecurity is a team sport within the department, and these efforts span many organizations. In particular, I work closely with General Alexander of Cyber Command in the definition and execution of the Department's cybersecurity program. I also work closely with each of the Services and Agencies and others in the Office of the Secretary of Defense to ensure cybersecurity issues are being addressed.

Given the complexity of the cybersecurity problem, and of DoD's IT environment, there are a wide range of technical and operational efforts aimed at achieving the above cybersecurity goals. Initiatives in support of the dependability and secrecy goals include efforts to remove vulnerability, to shield latent vulnerabilities by layering defenses, and to ensure an understanding of where vulnerabilities still exist. In spite of best efforts to harden DoD systems, an adversary may still succeed, so there are also a variety of efforts to contain, dampen, detect, diagnose, and react to successful or partially successful cyber intrusions and attacks.

A key priority in the last year has been the development of a unifying, joint cybersecurity approach for the design of the JIE. This is the JIE Single Security Architecture (SSA). Although many of the DoD's cyber security initiatives are common across all DoD organizations, each military service has had the ability to make important decisions about how to design computing and networks and about how to structure cyber defenses. This has led to several challenges, such as diversity in the cybersecurity protections of the DoD that does not provide a common level of protection for joint missions (because the IT for these missions is designed and operated by many organizations), and sometimes interferes with the collaborative attack detection, diagnosis, and reaction so necessary in a complex organization like DoD . Finally, the challenge caused by this diversity can interfere with a joint commander's ability to share information with external mission partners.

To solve these problems, the SSA provides for a common approach to the structure and defense of computing and the networks across all DoD organizations. For example, the SSA describes how core DoD data centers and the server computing they contain must be structured, what cyber defenses are required on these computers; what cyber "firebreaks" are necessary as part the internal networks of the data center; how remote management and automation of the data center is to be structured and secured; and what cyber-attack detection, diagnosis, and reaction

capabilities the data center and the remote management system must have. As another example, the SSA defines the structure of the computing and networks on a typical military base. A part of this is that all computer servers that must be located close to end-users (for example print servers) will be located in an installation processing node data center. The computers in this node must be configured and managed to DoD-wide cybersecurity standards and use DoD standard defense and situational awareness tools, and the installation processing node must be outfitted with perimeter defenses that can be configured to meet DoD wide policies. All information about this computing node and its defenses must be shared throughout the joint DoD cyber defense operational structures. A final example is that the SSA requires that the cyber identity credentials from the DoD Public Key Infrastructure (PKI) be used in every access to information in the JIE so as to drive anonymity out of the DoD networks, and it defines how directories that are used in access control decisions must be structured so as to strongly inhibit a cyber adversary's ability to move laterally inside the Department's networks.

This engineering of the cyber security approach "end-to-end" will significantly improve DoD's ability to resist cyber-attacks; to dampen the spread of successful attacks; and to detect, diagnose, and react to attacks in ways that are optimized for joint missions. Owing to the standardization and cyber data sharing of JIE, cyber defenders will have broad visibility into the computing and networks, and via secure remote management and automation, they will be able to much more quickly construct and execute defensive actions. In addition, the risk containment zones the SSA defines in the server computing and the network will enable joint commanders to better contain cyber risk to mission while sharing as broadly with external partners as a mission requires. It will also make development of new decision support capabilities simpler and easier since many program offices will not need to worry about most cybersecurity protections, but will instead be able to build software applications on top of the standard protections and situational awareness capabilities provided by JIE.

Public Key Infrastructure (PKI)

My introduction mentioned the DoD PKI cyber identity credential that is stored on our DoD Common Access Card (CAC) and is used by every DoD user on the unclassified networks. We are also deploying similar cyber identity credentials throughout the Department's Secret networks. This is a central part of efforts to drive anonymity out of the networks, and to drive up

the accountability required for a successful insider threat management program. To date, more than 300,000 smart cards with these PKI credentials have been issued and implementation efforts have begun for cryptographic logon for accounts using these credentials.

The government's secret networks are interconnected to improve interagency sharing of mission essential information. Standardization of the defenses of all of these networks is essential to the security of every agency, including DoD. To help other agencies more quickly drive out anonymity on the secret networks, and to drive up accountability in a cross-organization way via the use of a standard cyber identity credential, in calendar year 2012 DoD initiated work with other federal departments and agencies to provide them the ability to issue PKI cyber identity credentials for the secret networks. DoD's PKI Common Service Provider (CSP) is funded by non-DoD departments and agencies via an OMB-coordinated, shared fee for service cost model and is scheduled to allow other agencies to start issuing PKI credentials in June 2013. This will not only help improve accountability for information access, but as DoD works with the rest of the Government will make interagency sharing safer and easier.

Supply Chain Risk Management

Progress continues in other areas of cyber security. First, 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 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. Mr. Frank Kendall, the Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)), and I jointly issued DoD policy in November 2012, which makes permanent the Department's policies to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or components. My office and the office of the USD(AT&L) oversee implementation of this policy and work closely with the Military Services and nine Defense Agencies, including DISA, NSA, the Defense Intelligence Agency, and the Defense Logistics Agency, to achieve full operating capability for the Department.

My office has undertaken efforts to take its lessons learned to the interagency as well. Representatives from this office and DHS worked with the Committee on National Security Systems (CNSS) to develop CNSS Directive 505 - Supply Chain Risk Management, which serves as the supply chain policy that applies to all national security systems within the federal government. DoD also is partnering with other Departments and agencies to explore approaches to managing supply chain risk within critical infrastructures, which are critical to executing DoD missions.

The Defense Industrial Base Cybersecurity/Information Assurance Program

The DoD operates a successful public/private cyber information sharing program that is a model for other government/industry cybersecurity efforts. It 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 provides two-way cyber information sharing to include classified threat information sharing by the government, with voluntary sharing of incident data by industry, as well as sharing of mitigation and remediation strategies, digital forensic analysis, and cyber intrusion damage assessments. As an example, the DoD provides fast analysis of malicious software reported by industry and quickly shares with the DIB CS/IA participants, and with the rest of the Federal Government, machine readable indicators of the attack that can very quickly be deployed to protect others against new and emerging threats detected by any of the participating companies. While threats cannot be eliminated, the DIB CS/IA program enhances each DIB participant's capabilities to mitigate the risk, thereby further safeguarding DoD information that resides on, or that transits, DIB unclassified networks. Building on this successful model, the DoD partnered with the Department of Homeland Security to put in place a means of using even more highly classified information to protect the networks of participating companies. Under the DIB Enhanced Cybersecurity Services (DECS) program, the government provides highly classified cyber threat information either directly to a DIB company or to the DIB company's Commercial Service Provider (CSP). This sensitive, government-furnished information enables these DIB companies, or the CSPs on behalf of their DIB customers, to counter additional types of malicious cyber activity. The CSPs provide the protections as a commercial fee-for-service offering; the government is not involved in the financial aspects of

the transaction between a CSP and the participating DIB company. DoD is the government point of contact for the participating DIB companies, through the DoD's DIB CS/IA Program. DHS is the government point of contact for participating CSPs, under the umbrella of DHS' Joint Cybersecurity Services Program (JCSP), a broader effort to protect U.S. critical infrastructure

Future of Cybersecurity.

Transforming cyber defenses and regaining the advantage against cyber adversaries will require new strategic imperatives, such as shifting from reactive to more pro-active cyber defense operations, and focusing a greater portion of cyber defense activities on adversary activities and intent. Currently, the approach to cyber defense is based primarily on policy compliance, hardening configurations, and patching vulnerabilities, which are necessary but not sufficient. As the DoD focuses on cyber defenses driven by intelligence about the potential adversary, this shift will enable improvements to detect, protect, and respond to the threat's quickly changing cyber tactics. The term "active cyber defense" describes this new approach, which is DoD's synchronized real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It operates at network speed by sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. Adversaries will discover they cannot single out and attack local units without bringing to bear broader DoD support from intelligence and cyber forces. Active cyber defense is a transformational capability in an early operational stage. DoD will refine and evolve its capabilities by leveraging advances in all aspects of cyber operations and integrating national, regional, and organizational cyber defenses into a coherent active cyber defense framework.

Support to the Warfighter

In my capacity as the Department's CIO, I am responsible for overseeing Presidential and Senior Leader Communications; Nuclear Command, Control, and Communications; and Continuity Communications. The Deputy Secretary of Defense recently established a Joint Systems Engineering and Integration Office (JSEIO) under my direction, through the Director of DISA, to manage issues across all three of these critical mission areas. This will ensure a focused end-to-end integration of requirements, configuration management, assessments, and architecture in this nationally critical mission area.

Related and complementary to this function, I co-chair, along with a representative from the Department of Homeland Security, the National Security/Emergency Preparedness (NS/EP) Communications Executive Committee as a forum with members from the Departments of State, Defense, Justice, Commerce and Homeland Security; the Office of the Director of National Intelligence; the General Services Administration; and the Federal Communications Commission. The forum is responsible for ensuring the Federal Government has the ability to communicate at all times and under all circumstances to carry out its most critical and time sensitive missions, and for recommending policy and advising the President on NS/EP communications issues.

Positioning, Navigation and Timing (PNT)

Space-based positioning, navigation and timing (PNT) provides crucial capability to military, civil, and commercial users worldwide. We are working to better integrate the services of the Global Positioning System (GPS) as the primary means of delivering PNT. Precise timing is a key enabler of cyberspace operations and a part of our nation's critical infrastructure. Our PNT architecture provides our nation and allies the ability to precisely navigate anywhere in the world while the precise timing part also enables network encryption, synchronization and integration of data networks within the communications and cyber enterprises. With this understanding, we are working, as a high priority, several infrastructure upgrades to protect this critical piece of cyber terrain.

Spectrum

Spectrum has become increasingly important not only to the Department's missions, but to consumers and the economy of the nation as a whole. The use of the electromagnetic spectrum continues to be a critical enabler of our warfighting capabilities and the Department's cyber operations. Defense leadership is cognizant and sensitive to the unprecedented spectrum demands resulting from the Department's increasing reliance on spectrum-dependent technologies and the rapid modernization of commercial mobile devices. Fully recognizing the linkages between national security and economic prosperity, the DoD is fully committed to the President's 500 MHz initiative to make spectrum available for commercial broadband use, the implementation of more effective and efficient use of this finite radio-frequency spectrum and

the development of solutions to meet these goals while ensuring national security and other federal capabilities are preserved.

To that end, 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. DoD already is proactively working with NTIA, other Administration partners, and industry to methodically evaluate spectrum bands, through established deliberate processes. One example is DoD's extensive efforts, actively working with industry, to assess the feasibility of sharing the 1755-1850 MHz band through the NTIA established working groups under the Commerce Spectrum Management Advisory Committee (CSMAC). The CSMAC working groups' effort is an example of an unprecedented collaboration between the DoD and the commercial industry to assess highly complex technical issues with a goal of ensuring practical and balanced spectrum repurposing decisions that are technically sound and operationally viable from a mission perspective. 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.

Satellite Communications

Over the past year, DoD CIO has established a framework for end-to-end management of the Department's Satellite Communications (SATCOM) enterprise. The work of my office with DISA and the Services has already allowed the Department to realize some benefit as we conclude our analysis of a Commercial SATCOM cost recovery model, implement a converged SATCOM Gateway architecture, establish a plan of action for the Presidential Nuclear Voice Conferencing system integration, and conduct an analysis of alternatives for future protected and narrowband SATCOM requirements. This is especially critical in the Asia Pacific rebalance as the vast oceanic expanse requires additional focus on communications infrastructure that is provided with these efforts.

Asia Pacific Rebalancing

To support the President's and SECDEF's Strategic Guidance to rebalance emphasis towards the Asia-Pacific region, the DOD CIO developed, and is executing, a detailed program of action and

milestones to improve command, control, communications and computer (C4) systems in this area of operation (ref: DOD CIO C4 Strategy Memorandum, 30 Jul 2012). This combined COCOM, Service, and Agency effort involves actions to improve coalition partner information sharing, strengthen existing C4 capabilities in the region, and to add new capabilities based on lessons learned from recent operations in the Middle East. Specific actions include increasing capacity and redundancy for Pacific satellite communications gateways, improving resiliency/throughput of existing communications nodes, adding emergency failover capabilities to support critical communications, enhancing cyber defense/situational awareness, building and improving coalition network capabilities, and implementing a common Joint Information Environment (JIE) to improve network effectiveness, efficiency and security in the Pacific theater.

Workforce Development

A very important element of the Department's cyber defense strategy is ensuring that the right workforce is in place. An initial response to the needs of the Department is the accelerated delivery of cyber personnel in 2013 and 2014. The Department is building a balanced and highly capable military cyber force designed to meet our joint warfighting requirements. As General Alexander has noted, the Department is establishing cyber mission teams to support the Combatant Commands. The Department is focused on recruiting, training and retraining the necessary workforce to defend U.S. national interests in cyberspace. The workforce must be properly sized and properly trained, and there must be career paths that encourage growth and development of cyber defense and related skills, such as system management, cyber mission management, and cyber operations. 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.

Complementing the Department's cyber defense workforce component, is an enterprise wide cybersecurity awareness program designed to empower every person in DoD with the knowledge, skills and training to make continuously improving cybersecurity decisions. This effort is shared with 22 civil federal agencies.

Information Technology Exchange Program (ITEP)

Section 1110 of the FY10 National Defense Authorization Act (Public Law 111-84) authorized DoD to establish a Pilot Program for the Temporary Exchange of IT Personnel, referred to as the ITEP pilot, which expires September 30, 2013. While there has been limited participation to date, the assignments thus far have been mutually beneficial to DoD and private industry, and DoD has found the authority provides a valuable tool for exchanging innovative ideas with industry.

The ITEP program allows DoD and industry to each experience the challenges each other faces in managing their IT acquisitions, infrastructure and security requirements, and to exchange best practices on these issues.

While the program has been slow to grow and has had limited participation, the internal policies and processes to implement it have been established, and a long term program would help foster DoD relationships with the private sector and sustain the program. To date, an IT Project Management assignment was completed by Vanguard Advisors, LLC, within the Office of the DoD Comptroller and we currently have an ongoing ITEP assignment from Cisco Systems Inc. within my office.

IT Investment Planning

Additional changes to Department processes are necessary to ensure adaptability to technological advances and an ability to 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. We are leading a group comprised of Comptroller and CAPE to look at innovative options for funding enterprise services. An interactive transition plan template that defines "owner-operator," transition costs and funding strategies was designed and implemented for collecting data associated with the first increment of JIE in Europe. This template will serve as the basis for an integrated cost model that will be used for future IT

investment planning efforts. These are the primary efforts that will assure that the Department is using every dollar most effectively.

Conclusion

Maintaining information dominance for the warfighter is critical to our national security. The efforts outlined above 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.

Hold until Release by the
House Armed Services Subcommittee on
Intelligence, Emerging Threats and Capabilities

STATEMENT BY
THE HONORABLE ELIZABETH A. MCGRATH
DEPUTY CHIEF MANAGEMENT OFFICER
DEPARTMENT OF DEFENSE

BEFORE THE
INTELLIGENCE, EMERGING THREATS AND
CAPABILITIES SUBCOMMITTEE
OF THE
HOUSE ARMED SERVICES COMMITTEE

13 MARCH 2013

Introduction

Chairman Thornberry, Congressman Langevin and members of the Subcommittee, I appreciate the opportunity to update you on the management of the Department of Defense's business operations, including our progress in the oversight and implementation of modern, interoperable defense business systems. The Department has always taken its duty to be an excellent steward of taxpayer dollars very seriously. As the DoD Deputy Chief Management Officer, I am the Secretary and Deputy Secretary of Defense's primary agent for integrating and improving our critical business operations. I am responsible for instituting a framework to define clear business goals, create meaningful performance measures, and align activities via repeatable processes. The purpose of DoD's overarching management agenda, and the focus of the work undertaken by my office, is to establish an effective, agile, and innovative business environment that is fiscally responsible. There are many on-going efforts that are crucial to achieving this agenda, including the definition and refinement of the end-to-end processes that comprise the Department's business operations and IT acquisition reform, both of which I discussed when I last testified two years ago before this committee. While I am pleased to be able to report progress in both of these areas since that time, much remains to be done and a number of other important initiatives have been started.

The Department's defense business systems support critical functions such as financial management, supply chain, contracting, healthcare, and military personnel and payroll. However, many of these systems are old and handle or exchange information in ways that do not readily support current standards. These systems need to be modernized or replaced to support the achievement of key business outcomes, such as auditability, and the Department must do a better job at delivering these modern capabilities on time and within budget. Success in this area requires the alignment of broad Departmental strategy, functional business area strategy, and organizational investment decisions, as well as appropriate acquisition approaches and oversight. It also requires the proactive identification of enterprise data and process standards that will help us achieve an effective, agile, and innovative business environment.

Over the past number of years, attention to DoD defense business systems modernization has steadily increased and Congress has been instrumental in shaping the governance framework and supporting processes that the Department uses to oversee these efforts. We are particularly thankful for the changes introduced through Section 901 of the Fiscal Year 2012 National Defense Authorization Act, which have been a catalyst for dramatic improvements.

Today, I will update you on our integrated business framework, which has resulted from these recent changes, the maturation of our business enterprise architecture, and some of our recent successes and challenges in the implementation of our largest IT systems.

Investment Management

Section 901 of the Fiscal Year 2012 National Defense Authorization Act, now codified at Title 10 United States Code § 2222, included significant changes to the requirements for investment review and certification of defense business systems before funds can be obligated. Continuing to build on existing statutory guidance that requires Business Process Reengineering (BPR) and alignment to the Business Enterprise Architecture (BEA), Section 901 required the establishment of a single Investment Review Board (IRB), chaired by the DoD Deputy Chief Management Officer (DCMO), and investment management process.

Section 901 also significantly expanded the scope of systems requiring certification to include any business system with a total cost in excess of $1 million over the period of the current future–years defense program, regardless of type of funding or whether any development or modernization is planned. In the prior IRB process, approximately $1.8 billion in funding was assessed and certified each year, covering only those systems that were actively being developed or modernized. The expanded scope in Section 901 will result in virtually all of the more than $7 billion annual business system information technology funding being assessed and certified.

To execute this new investment management process, the DCMO issued guidance that established a portfolio-based approach with several key elements and chartered a new governance body, the Defense Business Council to serve as the Department's single IRB. The Defense Business Council has successfully brought together and integrated the efforts of a number of existing governance bodies to provide a single forum in which to manage DoD business operations from the creation of our overarching business management strategy to implementation of the strategy's underlying programs and initiatives.

As part of this portfolio-based investment management approach, each year, Functional Strategies, aligned with the Department's Strategic Management Plan (SMP), are created by the appropriate business line owner that provide guidance to DoD Components on the strategic vision, goals, priorities, outcomes, measures, and any mandatory enterprise solutions for a given functional area (e.g., financial management, human resources, etc.). Organizational Execution Plans are then developed by DoD

Components (e.g., Military Departments, Defense Agencies, etc.) that include details on the Component's proposed business system investments, such as their alignment with the Department's functional strategies and their adherence to BPR and BEA requirements. The Organizational Execution Plans also demonstrate cross functional integration and articulate any other mission imperatives of the Component. Then, the Defense Business Council, which is comprised of senior business representatives from across the Department, reviews the proposed investments and the DCMO, as chair of the Defense Business Council, approves the Organizational Execution Plan certifications, recording the outcomes in decision memoranda.

The Department's new investment management process ensures that investments are aligned to strategies, allows the Department to make more informed investment decisions, eliminates legacy systems that are no longer required, enhances interoperability, and helps the Department transform to an environment where business applications are able to be rapidly deployed on a common computing infrastructure. The process also ensures that each investment is an appropriate use of taxpayer dollars and meets our shared goal of delivering agile, effective and efficient business solutions that support and enable our warfighters. The certification process that we went through for Fiscal Year 2013, for example, identified approximately 10% of the systems reviewed as legacy systems that would be retired over the next three years. Steps have been taken to ensure that those systems will actually be terminated.

The Department is now in the midst of the process of certifying investments for Fiscal Year 2014. The SMP, which is the Department's highest-level plan for improving business operations and is designed to align all business goals and operations for the Department of Defense, has been updated and a new version will be issued early this spring. New Functional Strategies are being written to align with this new strategic guidance and will provide implementation details needed to achieve the goals of the SMP. Then, as we move through the spring and into the summer, new Organizational Execution Plans will be compiled and reviewed by the Defense Business Council. This new investment management process allows the Department, for the first time, to more holistically manage our entire portfolio of business systems in a deliberate and organized manner, including our legacy systems that are in sustainment, and is truly serving as a catalyst for dramatic improvements.

Business Enterprise Architecture

One of the key supporting elements of the Department's improved, portfolio driven, and strategically aligned investment management process is the Business Enterprise Architecture. The purpose of the Business Enterprise Architecture is to

provide a blueprint for DoD business transformation that helps ensure the right capabilities, resources and materiel are rapidly delivered to our warfighters – what they need, where they need it, when they need it, anywhere in the world. The Business Enterprise Architecture does this by articulating the data standards, business rules, laws, regulations, and policies that are needed to effectively execute the Department's end-to-end processes and that DoD business system investments must adhere to.

The Business Enterprise Architecture's content is driven by and aligned with the Strategic Management Plan, Functional Strategies, and Organizational Execution Plans and it, in turn, drives the content of those documents as well. Together, these documents and the processes that support them enable the Department to make wise investment decisions that track from top level strategy all the way down to individual system execution. It also guides information technology investment management to align with strategic business capabilities as required by the Clinger-Cohen Act, and supporting Office of Management and Budget (OMB) and Government Accountability Office (GAO) policies. On February 14, 2013, the Department issued Business Enterprise Architecture Version 10.0. This new release makes important improvements to previous releases both in its structure and in its content.

Defense Business Systems Successes and Challenges

As I've outlined, the Department has continued to mature its governance processes and its architectural framework. These strides forward are extremely important, foundational improvements. However, they will only be judged successful if they can effectively enable better system implementations and business outcomes.

Some of the Department's most visible defense business system implementations are our Enterprise Resource Planning systems (ERPs), both because of their sheer size and also because of the challenges that they have experienced over the years. Today, DoD is implementing multiple ERPs across the Military Departments and Defense Agencies to serve as the business backbone for our operations. Each of these implementations is at a different stage in its lifecycle and most have experienced challenges as they have moved from design to implementation. Broadly, we continue to improve our oversight of these programs in a number of ways, including putting in place more rigorous performance measures that broaden the discussion from standard acquisition measures to key technical and business measures. This has led to a closer link between the information technology programs and the business outcomes that they are helping to enable. Additionally, we are applying lessons learned across all of the programs in the portfolio. We are also incorporating recent GAO and DoDIG findings, which have highlighted deficiencies in compliance, shortcomings in change management

or training and difficulties in management of data quality and interfaces that have created inefficiencies and labor intensive rework. We acknowledge that there have been and continue to be issues and, as GAO has noted, DoD governance has taken appropriate action to limit the pace of deployment. We are committed to working through every significant deficiency in order to realize the long term value of these investments.

Over the past 6 months, I have undertaken a substantial effort to fully understand and define the leading root causes of a program's success along the dimensions of cost, schedule, and performance. We have discovered some key findings:

- Much of a program's probability of success may be predicted early in the acquisition lifecycle, often before a request for proposal (RFP) is released.
- Focusing the Department on quality, upfront work in three areas can significantly improve program outcomes:
    - Ensuring clarity of the program's scope and requirements.
    - Testing for completeness and conducting a thorough Analysis of Alternatives.
    - Developing a quantifiable business case.
- Across the lifecycle of a program, six critical leading indicators (identified and vetted with both private and public business sector stakeholders) can inform programs' success trajectory:
    - Is the design of the program clear (objectives, requirements, technical details, and investment case) to ensure consistent understanding across stakeholders and vendors?
    - Is the program robustness enough to encounter problems or issues and remain a positive investment for the government?
    - Are program increments/requirements severable from one another to ensure the Department's Return on Investment (ROI) is delivered across the program's lifecycle?
    - Is the design of the program stable enough to minimize changes in development and prevent a ripple effect across the program?
    - Are program dependencies with other requirements, systems, or data sources identified up front to ensure program success?
    - Is accountability clear to ensure various stakeholders are aligned and recognize and communicate critical messages required for decision makers?

In recognition of these findings, I have taken the following actions:

- Implemented increased emphasis on the use of the Business Capability Lifecycle (BCL) alternative acquisition process for defense business systems to apply more rigor and consistency to programs throughout the lifecycle phases.
- Formalized a problem statement review process within the Defense Business Council to strengthen rigor in the earliest phase of a program by requiring comprehensive business cases to justify IT functionality provided by large programs.
- Undertaken reviews of large, MAIS/ACAT-1 business systems to identify the root cause drivers of program issues (and the downstream effects) at every stage in the lifecycle. Reviews are conducted at the DCMO portfolio level as well as at-the-ground level within multiple programs.
- Commissioned an effort to establish a performance management structure that measures "leading indicators" of program success to help predict / prevent a program from incurring cost increases or delays.
- Begun piloting "leading indicators" in my current program portfolio to strengthen each program's success trajectory.

My next steps include:

- Continue to examine the process by which we scope large programs – manageable increments which deliver capability in shorter development cycle.
- Continue to roll out the "leading indicators" across the Department's IT portfolio to aid in the determination if programs are set up for success and assist program teams to focus on key program attributes (e.g., requirement clarity) that drive success.
- Conduct an analysis of unsuccessful programs to leverage findings into future programs to prevent similar issues.

Conclusion

In closing, the Department is committed to improving the management and acquisition of IT systems, as well as our overarching business operations. These issues receive significant management attention and are a key part of our broad strategy to build better business processes that will create lasting results for our men and women in uniform and the American taxpayer. I look forward to continuing our work with this committee in the months and years ahead and being able to report additional gains in our quest for greater efficiency, increased effectiveness, and further agility, enabled by modern, interoperable IT capabilities.

I look forward to your questions.

Elizabeth A. McGrath

Deputy Chief Management Officer for Department of Defense

Ms. Elizabeth (Beth) McGrath is the Department of Defense Deputy Chief Management Officer and the Department's Performance Improvement Officer. In these roles, Ms. McGrath leads the Department's effort to better synchronize, integrate, and coordinate Department of Defense (DoD) business operations and serves as the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary of Defense for matters relating to management and the improvement of business operations. Ms. McGrath is focused on achieving an effective, agile and innovative business environment across the Department's enterprise that promotes sustainability, transparency and fiscal responsibility.

Ms. McGrath is responsible for generating the DoD Strategic Management Plan; administering the DBSMC, the Department's primary governance body for overseeing business operations; establishing performance goals and measurements for the Department's business functions; and implementing DoD's Continuous Process Improvement. She serves as the vice chair of the Federal Performance Accountability Council overseeing government-wide security clearance process reform initiatives, and leads the Department's effort on the joint integrated Electronic Health Record initiative with the Department of Veterans Affairs. Ms. McGrath retains acquisition decision authority over a $3 billion information technology (IT) business system portfolio and investment management responsibility for an additional $4 billion business IT systems/initiatives. Her role as DCMO requires integration and coordination across DoD and other inter-governmental agencies to include the Office of Management and Budget and the Government Accountability Office.

Previously, Ms. McGrath served as the Deputy Director for Systems Integration, Defense Finance and Accounting Service (DFAS) where she created a financial migration strategy that included a comprehensive architecture and identification of DoD-wide systems valued at more than $1 billion.

Prior to joining DFAS, Ms. McGrath served in a variety of Program Management roles culminating in Program Executive Office (PEO) level oversight responsibility. She possesses extensive knowledge of acquisition-related statutes, regulations and policies and more than 20 years applied acquisition experience with Major Defense Acquisition Programs (MDAP) and Major Automated Information Systems (MAIS). She served as the Business and Acquisition Manager on an international program with the United Kingdom and held numerous other financial, acquisition and program management positions within the US Department of the Navy.

Ms. McGrath holds a B.S. degree in Economics from George Mason University and is a graduate of the Federal Executive Institute (FEI). She is certified Acquisition Level III in Program Management, Financial Management and Logistics, is a member of the DoD Acquisition Professional Community, and a member of the National Academy of Public Administration. Her awards include: National Intelligence Meritorious Unit Citation, Presidential Rank Award, Office of the Secretary of Defense Exceptional Civilian Service Medal, and DoD Medal for Distinguished Public Service. She has been recognized by Government Computer News with the Defense IT Executive of the Year award and has also received multiple Federal 100 awards.

STATEMENT OF

GENERAL KEITH B. ALEXANDER

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

INTELLIGENCE, EMERGING THREATS AND CAPABILITIES SUBCOMMITTEE

13 MARCH 2013

Thank you very much Chairman Thornberry and Ranking Member Langevin for inviting me to speak to you and your colleagues today on behalf of the men and women of U.S. Cyber Command. I have the honor of leading them on a daily basis, and let me assure you there is not a finer and more dedicated team of Service members and civilian personnel anywhere. It gives me great pleasure to appear before you to talk about their accomplishments, and to describe some of the challenges they face in performing their difficult but vital mission of keeping U.S. military networks secure, helping to protect our nation's critical infrastructure from national-level cyber attacks, assisting our Combatant Commanders around the world, and working with other U.S. Government agencies tasked with defending our nation's interests in cyberspace.

USCYBERCOM is a subunified command of U.S. Strategic Command in Omaha, though we are based at Fort Meade, Maryland. We have approximately 834 active-duty military and civilians assigned from an authorized end-strength of 917 (plus contractors), and a budget of approximately $191 million for Fiscal Year 2013. USCYBERCOM has strong, evolving, and growing cyber components representing each of the Services: Fleet Cyber Command/Tenth Fleet, Army Cyber Command/Second Army, Air Force Cyber Command/24th Air Force, and Marine Forces Cyber Command. Each of our Service Cyber Components also has representation at our headquarters. Combined we and they have more than 11,000 people in our force mix.

US Cyber Command shares its headquarters with key mission partners in the National Security Agency (NSA), which I also lead. USCYBERCOM's co-location with NSA promotes intense and mutually beneficial collaboration. The Department of Defense established U.S. Cyber Command in 2010 to leverage NSA's capabilities. This partnership is key to what we are doing now, and provides the essential context for all the activities I shall describe below. The people under my command and direction at USCYBERCOM and NSA are collectively responsible for operating the Department's information networks, detecting threats in foreign cyberspace, attributing threats, securing national security and military information systems, and helping to ensure freedom of action for the United States military and its allies in cyberspace—and, when directed, defending the nation against a cyber attack. Also nearby at Fort Meade is another key mission partner, the Defense Information Systems Agency (DISA). The constellation of agencies and capabilities in the Washington DC region makes for a unique synergy of people and ideas—a nexus for military and national cybersecurity innovation.

USCYBERCOM has deployed representatives and mission support elements worldwide. We have an expeditionary cyber support unit forward in

Afghanistan. We also have liaison officers at each Combatant Command (serving as that Command's CSE lead) and in several other key offices and agencies in the Washington area. The flow of information and advice across USCYBERCOM and its Service components and the commands, agencies, and foreign mission partners here and overseas is improving slowly but steadily.

Since I last spoke with you in March 2012, our progress has accelerated. In December we moved ahead with building a balanced and highly capable military cyber force designed to meet our joint warfighting requirements. We have laid out and codified team composition, training, and certification standards to field a world-class force in support of the Combatant Commands (CCMDs). Although we have much work to do, we are focused on doing it right and meeting the CCMDs' and the nation's most pressing cyber defense requirements. In short, we have moved ahead to normalize cyber operations within the U.S. military, and to turn that capability into a reliable option for decisionmakers to employ in defending our nation. This progress will not only make our military more capable but our networks and information more secure. We have serious threats facing us, as I shall explain. Our progress, however, can only continue if we are able to fulfill our urgent requirement for sufficient trained, certified, and ready forces to defend U.S. national interests in cyberspace.

The Strategic Landscape

U.S. Cyber Command operates in a dynamic and contested environment that literally changes its characteristics each time someone powers on a networked device. Geographic boundaries are perhaps less evident in cyberspace, but every server, fiber-optic line, cell tower, thumb drive, router, and laptop is owned by someone and resides in some physical locale. In this way cyberspace resembles the land domain—it is all owned, and it can be re-shaped. Most networked devices, for example, are in private hands, and their owners can deny or facilitate others' cyber operations by how they manage and maintain their networks and devices. Cyberspace as an operating environment also has aspects unique to it. Events in cyberspace can seem to happen instantaneously. Data can appear to reside in multiple locations. There is a great deal of anonymity, and strongly encrypted data are virtually unreadable. In cyberspace, moreover, sweeping effects can be precipitated by states, enterprises, and individuals, with the added nuance that such cyber actors can be very difficult to identify. The cyber landscape also changes rapidly with the connection of new devices and bandwidth, and with the spread of strong encryption and mobile devices. Despite the unique characteristics of cyberspace, states still matter because they can affect much of the physical infrastructure within their borders. Convergence is our watchword; our communications, computers, and networks are merging into one digital

environment as our political, economic, and social realms are being re-shaped by the rush of innovation.

In this environment that is both orderly and chaotic, beneficial and perilous, we at USCYBERCOM have to focus on actors who possess the capability—and possibly the intent—to harm our nation's interests in cyberspace or to use cyber means to inflict harm on us in other ways. Unfortunately, the roster of actors of concern to us is growing longer and growing also in terms of the variety and sophistication of the ways they can affect our operations and security.

State actors continue to top our list of concerns. We feel confident that foreign leaders believe that a devastating attack on the critical infrastructure and population of the United States by cyber means would be correctly traced back to its source and elicit a prompt and proportionate response. Nonetheless, it is possible that some future regime or cyber actor could misjudge the impact and the certainty of our resolve.

We have some confidence in our ability to deter major state-on-state attacks in cyberspace but we are not deterring the seemingly low-level harassment of private and public sites, property, and data. As former Secretary of Defense Panetta explained to an audience in New York last October, states and extremist groups are behaving recklessly and aggressively in the cyber environment. Such attacks have been destructive to both data and property. The Secretary mentioned, for example, the remote assaults last summer on Saudi Aramco and RasGas, which together rendered inoperable—and effectively destroyed the data on—more than 30,000 computers. We have also seen repressive regimes, desperate to hold on to power in the face of popular resistance, resort to all manner of cyber harassment on both their opponents and their own citizens caught in the crossfire. Offensive cyber programs and capabilities are growing, evolving, and spreading before our eyes; we believe it is only a matter of time before the sort of sophisticated tools developed by well-funded state actors find their way to non-state groups or even individuals. The United States has already become a target. Networks and websites owned by Americans and located here have endured intentional, state-sponsored attacks, and some have incurred damage and disruption because they happened to be along the route to another state's overseas targets.

Let me draw your attention to another very serious threat to U.S. interests. The systematic cyber exploitation of American companies, enterprises, and their intellectual property continued unabated over the last year. Many incidents were perpetrated by organized cybercriminals. Identity and data theft are now big business, netting their practitioners large profits and giving rise to an on-line sub-culture of markets for stolen data and cyber tools for stealing more. Much cyber exploitation activity, however, is state-sponsored. Foreign government-directed cyber collection personnel, tools, and

organizations are targeting the data of American and western businesses, institutions, and citizens. They are particularly targeting our telecommunications, information technology, financial, security, and energy sectors. They are exploiting these targets on a scale amounting to the greatest unwilling transfer of wealth in history. States and cybercriminals do not leave empty bank vaults and file drawers behind after they break-in—they usually copy what they find and leave the original data intact—but the damage they are doing to America's economic competitiveness and innovation edge is profound, translating into missed opportunities for U.S. companies and the potential for lost American jobs. Cyber-enabled theft jeopardizes our economic growth. We at USCYBERCOM work closely with our interagency partners to address these threats.

We must also watch potential threats from terrorists and hacktivists in cyberspace. The Intelligence Community and others have long warned that worldwide terrorist organizations like al Qaeda and its affiliates have the intent to harm the United States via cyber means. We agree with this judgment, while noting that, so far, their capability to do so has not matched their intent. This is not to downplay the problem of terrorist use of the Internet. Al Qaeda and other violent extremist groups are on the Web proselytizing, fundraising, and inspiring imitators. We should not ignore the effectiveness with which groups like al Qaeda and its affiliates radicalize ever larger numbers of people each year—on more continents. The Federal Bureau of Investigation and other agencies cite instances in which would-be terrorists found motivation and moral support for suicide attacks at jihadist websites and chat rooms. This is an especially serious and growing problem in areas of hostilities where our troops and personnel are deployed. Another threat that is not growing as fast as we might have feared, on the other hand, is that of hacktivists with a cause or a grievance that leads them to target U.S. government and military networks. Our vulnerabilities to this sort of disruption remain, but 2012 saw fewer such incidents than 2011.

Looking Ahead: The Command's Priorities

I have established several priorities for U.S. Cyber Command in dealing with these risks and threats. We are actively working to guard the Department of Defense's networks and information and helping to defend the nation. Key to countering these threats is learning <u>how</u> to grow our capabilities in this challenging domain. We have no alternative but to do so because every world event, crisis, and trend now has a cyber-aspect to it, and decisions we make in cyberspace will routinely affect our physical or conventional activities and capabilities as well. USCYBERCOM is building cyber capabilities into our planning, doctrine, and thinking now—while we as a nation have time to do so in a deliberate manner. We do not want to wait for a crisis and then have to respond with hasty and ad hoc solutions that could do more harm than good.

When I say we are normalizing cyber operations, I mean we are making them a more reliable and predictable capability to be employed by our senior decisionmakers and Combatant Commanders. Normalizing cyber requires improving our tactics, techniques, and procedures, as well as our policies and organizations. It also means building cyber capabilities into doctrine, plans, and training – and building that system in such a way that our Combatant Commanders can think, plan, and integrate cyber capabilities as they would capabilities in the air, land and sea domains.

In keeping with the Department of Defense's *Strategy for Operating in Cyberspace*, U.S. Cyber Command and NSA are together assisting the Department in building: 1) a defensible architecture; 2) global situational awareness and a common operating picture; 3) a concept for operating in cyberspace; 4) trained and ready cyber forces; and 5) capacity to take action when authorized. Indeed, we are finding that our progress in each of these five areas benefits our efforts in the rest. We are also finding the converse—that inertia in one area can result in slower progress in others. I shall discuss each of these priorities in turn.

Defensible Architecture: The Department of Defense (DoD) owns seven million networked devices and thousands of enclaves. Cyber Command works around the clock with its Service cyber components, with NSA, and with DISA to monitor the functioning of DoD networks, including the physical infrastructure, the configurations and protocols of the components linked by that infrastructure, and the volume and characteristics of the data flow. This is a dynamic defense, and it consistently provides better security than the former patch-and-firewall paradigm. Patches and firewalls are still necessary—I wish everyone kept theirs up-to-date—but they are an insufficient defense for DoD networks. Dynamic defenses have brought about noticeable improvements in the overall security of DoD information environment. We know for a fact that our adversaries have to work harder to find ways into our sensitive but unclassified networks. Unfortunately, adversaries are willing to expend that effort, and DoD's architecture in its present state is not defensible over the long run. We in the Department and the Command are crafting a solution. The Department's bridge to the future is called the DoD Joint Information Environment (JIE), comprising a shared infrastructure, enterprise services, and a single security architecture to improve mission effectiveness, increase security, and realize information technology (IT) efficiencies. The JIE will be the base from which we can operate in the knowledge that our data are safe from adversaries. Senior officers from USCYBERCOM and NSA sit on JIE councils and working groups, playing a leading role with the office of the DoD's Chief Information Officer, Joint Staff J6, and other agencies in guiding the Department's implementation of the JIE. NSA, as the Security Adviser to the JIE, is defining the security dimension of that architecture, and has shown how we can pool big data and still preserve strong security. We have even

shared the source code publicly so public and private architectures can benefit from it. DoD is benefitting from that knowledge and from our growing understanding of the totality of measures, procedures, and tools required to assure the health and security of even the biggest networks and databases.

Increased Operational Awareness: Enhanced intelligence and situational awareness in our networks will help us know what is happening in the cyberspace domain. This effort can be likened to a cyber version of the tactical air picture of friendly, neutral, and aggressor aircraft that a Combined Air Operations Center in a Combatant Command typically maintains. We are now issuing a weekly Cyber Operating Directive (CyOD) across the DoD cyber enterprise for just this purpose, so that all "friendlies" understand what is happening in cyberspace. Our improving knowledge of what is normal in cyberspace is crucial to grasping what is not normal. We at USCYBERCOM are also helping DoD increase our global situational awareness through our growing collaboration with federal government mission partners like the Department of Homeland Security (DHS), the FBI, and other departments and agencies, as well as with private industry and with other countries. That collaboration in turn allows us to better understand what is happening across the cyber domain, which enhances our situational awareness, not only for the activities of organizations based at Fort Meade but also across the U.S. government. I am happy to report that at least one of our foreign partners has volunteered to invest in this and enter its own network traffic data to contribute to a common picture.

Operating Concepts: Our operating concept calls for us to utilize our situational awareness to recognize when an adversary is attacking, to block malicious traffic that threatens our networks and data, and then to maneuver in cyberspace to block and deter new threats. I am pleased to report that in December, the Department endorsed the force presentation model we need to implement this new operating concept. We are establishing cyber mission teams in line with the principles of task organizing for the joint force. The Services are building these teams to present to U.S. Cyber Command or to support Service and other Combatant Command missions. The teams are analogous to battalions in the Army and Marine Corps—or squadrons in the Navy and Air Force. In short, they will soon be capable of operating on their own, with a range of operational and intelligence skill sets, as well as a mix of military and civilian personnel. They will also have appropriate authorities under order from the Secretary of Defense and from my capacity as the Director of NSA. Teams are now being constructed to perform all three of the missions given to U.S. Cyber Command. We will have 1) a Cyber National Mission Force and teams to help defend the nation against national-level threats; 2) a Cyber Combat Mission Force with teams that will be assigned to the operational control of individual Combatant Commanders to support their objectives (pending resolution of the cyber command and control model by the

Joint Staff); and 3) a Cyber Protection Force and teams to help operate and defend DoD information environment.

Trained and Ready Forces: Each of these cyber mission teams is being trained to common and strict operating standards so that they can be on-line without putting at risk our own military, diplomatic, or intelligence interests. Doing this will give not only U.S. Cyber Command's planners, but more significantly our national leaders and Combatant Commanders, a certain predictability in cyber capabilities and capacity. Key to building out the Cyber Mission Force articulated in our Force Planning Model is having the training system in place to train each of the cyber warriors we need, in the skill sets we require and at the quality mandated by the cyber mission. We have that training system in place for the operators, and now we need to build the accompanying Command and Staff academic support packages and programs to ensure our officers and planners know how to effectively plan for and employ cyber capabilities for our nation. As a result of this operator and staff training system, decisionmakers who require increments of cyber skills to include in their plans will know how to ask for forces to fill this requirement, and planners will know how to work cyber effects into their organizations' plans. To build the skills of the force—as well as to test the ways in which its teams can be employed—U.S. Cyber Command has sponsored not only an expanding range of training courses but also two important exercises, CYBER FLAG and CYBER GUARD. The latter assembled 500 participants last summer including a hundred from the National Guards of twelve states. They exercised state and national-level responses in a virtual environment, learning each other's comparative strengths and concerns should an adversary attack our critical infrastructure in cyberspace. CYBER FLAG is our annual exercise at Nellis Air Force Base in Nevada and we conduct it with our inter-agency and international partners. Our most recent running of CYBER FLAG introduced new capabilities to enable dynamic and interactive force-on-force maneuvers at net-speed, while incorporating actions by conventional forces as well at Nellis' nearby training area.

Capacity to Take Action: Successful operations in cyberspace depend on collaboration between defenders and operators. Those who secure and defend must synchronize with those who operate, and their collaboration must be informed by up-to-date intelligence. I see greater understanding of the importance of this synergy across the Department and the government. The President recently clarified the responsibilities for various organizations and capabilities operating in cyberspace, revising the procedures we employ for ensuring that we act in a coordinated and mutually-supporting manner. As part of this progress, the Department of Defense and U.S. Cyber Command are being integrated in the machinery for National Event responses so that a cyber incident of national significance can elicit a fast and effective response to include pre-designated authorities and self-defense actions where necessary and appropriate. USCYBERCOM is also working with the Joint Staff and the

Combatant Commands to capture their cyber requirements and to implement and refine interim guidance on the command and control of cyber forces in-theater, ensuring our cyber forces provide direct and effective support to commanders' missions while also helping U.S. Cyber Command in its national-level missions. In addition, we are integrating our efforts and plans with Combatant Command operational plans and we want to ensure that this collaboration continues at all the Commands. Finally, most cyber operations are coalition and interagency efforts, almost by definition. We gain valuable insight from the great work of other partners like the Departments of Justice and Homeland Security, such as in their work against distributed denial of service attacks against American companies, which in turn helps DoD fine-tune defenses for the DoD information environment. We also benefit from sharing with the services and agencies of key partners and allies. We welcome the interagency collaboration and evolving frameworks under which these efforts are proceeding, especially such revisions that would make it easier for the U.S. Government and the private sector to share threat data, as the administration previously emphasized. In addition, new standing rules of engagement for cyber currently under development will comply with and support recently issued policy directives on U.S. cyber operations.

Building for the Future

We have made strides in all of our focus areas, though what gratifies me the most is seeing that we are learning how they all fit together. We are building quickly and building well, but we are still concerned that the cyber threats to our nation are growing even faster. From the technological, legal, and operational standpoints we are learning not only what is possible to accomplish but also what is wise to attempt. Our plans for U.S. Cyber Command over the foreseeable future—which admittedly is not a very distant horizon—should be understood in this context.

In a speech last fall, then-Secretary Panetta emphasized the Department's need to adjust our forces as we transition away from a decade of war. He explained that a wise adjustment makes cuts without hollowing out the force, while also investing in ways that prepare us to meet future needs. We will do that, he said, by increasing our investments in areas including space and cyber. It is fair to ask how we plan to use such new resources while others are trimming back. Our new operating concept to normalize cyber capabilities is just the sort of overarching theme to unite the whole institutional push. We need to foster a common approach to force development and force presentation—up to and including the Service component and joint headquarters—given the intrinsically joint nature of this domain.

Let me emphasize that this is not a matter of resources alone – it is a matter of earning trust. We will continue to do our work in full support and defense of the civil liberties and privacy rights enshrined in the U.S. Constitution. We do not see a tradeoff between security and liberty. We can and must promote both simultaneously because each enhances the other. U.S. Cyber Command takes this responsibility very seriously. Indeed, we see this commitment in our day-by-day successes. We in the Department of Defense and DHS, with DOJ and industry, for instance, have shown that together we can share threat information, to include malware signatures, while still providing robust protection for privacy and civil liberties..

Building the Department's defensible cyber architecture will let us guard our weapons systems and military command and control as well as our intelligence networks. We hope to take the savings in personnel and resources gained by moving to the JIE and have the Services repurpose at least some of them to hunt for adversaries in our DoD networks and even to perform full-spectrum operations. Although doing so will require a large investment of people, resources, and time, in the long run it will be cheaper to train Service personnel than to hire contractors. Moving to the JIE will make sharing and analytics easier while also boosting security. I know this sounds paradoxical but it is nonetheless true, as NSA has demonstrated in its Cloud capability. If we know what is happening on our networks, and who is working in them and what they are doing, then we can more quickly and efficiently see and stop unauthorized activities. We can also limit the harm from them and more rapidly remedy problems, whether in recovering from an incident or in preventing one in the first place. This is our ultimate objective for operations on our Department of Defense information architecture.

As we grow capacity, we are building cyber mission teams now , with the majority supporting the Combatant Commands and the remainder going to USCYBERCOM to support national missions. When we have built this high-quality, certified, and standardized force, we will be able to present cyber forces with known capability sets to our Combatant Commanders—forces they can train with, plan for, plan on, and employ like forces and units any other military domain. This gets at the essence of normalizing cyber capabilities for the Department of Defense. Furthermore, we want to increase the education of our future leaders by fully integrating cyber in our existing war college curricula. This will further the assimilation of cyber into the operational arena for every domain. Ultimately we could see a war college for cyber to further the professional military education of future leaders in this domain.

Conclusion

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to speak to you today. I hope you will agree with me that U.S.

Cyber Command has made progress across the board in the last year, thanks to the support of Congress and our interagency and international partners, as well as the hard work of its many dedicated men and women. The novelist and visionary William Gibson once noted "The future is already here, it's just not evenly distributed." We are seeing that future at U.S. Cyber Command. Cyber capabilities are already enhancing operations in all domains. We are working to contain the vulnerabilities inherent in any networked environment or activity while ensuring that the benefits that we gain and the effects we can create are significant, predictable, and decisive. If I could leave you with one thought about the course of events, it is that we have no choice but to normalize cyberspace operations within the US military and make them part of the capability set of our senior policymakers and commanders. I am ready to take your questions and to clarify our Command's achievements and challenges, and to discuss any concerns that you might wish to share.

Biography - Commander, U.S. Cyber Command, Director, National Security Agency/Chief, Central Security Service

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.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

MARCH 13, 2013

RESPONSE TO QUESTION SUBMITTED BY MR. THORNBERRY

Ms. TAKAI. Response to DSB Report on Resiliency:

The Defense Science Board (DSB) report entitled, "Resilient Military Systems and the Advanced Cyber Threat" makes a series of recommendations. There is significant effort in the CIO, USCYBERCOM, and NSA mission spaces already happening or planned in each recommendation area. Below are short summaries of the major DSB recommendations, and examples of ongoing and planned work to meet them. This list does not include efforts outside of the CIO/USCYBERCOM/NSA area of responsibility.

DSB Recommendation #1: Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary (DSB report page 7).

Secretary of Defense assign United States Strategic Command the task to ensure the availability of Nuclear Command, Control and Communications ([N]C3) and the Triad delivery platforms in the face of a full-spectrum Tier V–VI attack—including cyber (supply chain, insiders, communications, etc.)

Examples of ongoing efforts

- Multi-level human intervention and off-line launch code authentications
- NSA-produced NC3 Information Assurance (IA) materials
- Stood up the Strategic and National C3 and Intelligence (SNC3I) Joint Systems Engineering & Integration Office (JSEIO) to do end-to-end engineering of NC3
- CIO & USD(AT&L) signed DODI 5200.44 which institutionalizes supply chain risk management in acquisition and sustainment
- CIO & USD(AT&L) assisting STRATCOM in application of supply chain risk management (SCRM) to its key programs

DSB Recommendation #2: Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary (DSB report page 7).

SECDEF and Chairman, Joint Chiefs of Staff (CJCS) designate a mix of forces necessary for assured operation.... Segment Sufficient Forces to Assure Mission Execution in a Cyber Environment

Examples of ongoing efforts

- Established Cyber National Mission Force-trained and certified teams
- Implementing the Joint Information Environment (JIE) to improve cyber defense and resilience of unclassified and secret networks for better protected conventional capabilities
- Increased funding for cyber capability development (on-hold for sequestration and Continuing Resolution)
- NSA collection and analysis critical to understanding adversary

DSB Recommendation #3: Refocus Intelligence Collection and Analysis to Understand Adversarial Cyber Capabilities, Plans and Intentions, and to Enable Counter-strategies (DSB report page 8). SECDEF in coordination with the Directors of CIA, FBI, and DHS, should require the Director of National Intelligence (DNI) to support enhanced intelligence collection and analysis on high-end cyber threats

Examples of ongoing efforts

- Improving threat information sharing in real-time across USG
- Increased Intelligence Community (IC)/NSA focus on cyberspace operations support
- Increased "hunting" on blue networks
- Cyber integrees from NSA/USCYBERCOM at FBI, CIA, and DHS; and vice versa

DSB Recommendation #4: Build and Maintain World-Class Cyber Offensive Capabilities (with appropriate authorities) (DSB report page 9).

United States Cyber Command (USCYBERCOM) develop capability to model, game and train for full-scale cyber warfare.

Under Secretary of Defense for Personnel and Readiness (USD(P&R)) establish a formal career path for civilian and military personnel engaged in offensive cyber actions.

Examples of ongoing efforts
- Established Cyber National Mission Force (Cyber National Mission Teams and Combatant Command Mission Teams)
- Cyberspace operations-focused training exercises (Cyber Flag, Cyber Guard, and Cyber Knight)
- CJCS cyber emergency action conferences

DSB Recommendation #5: Enhance Defenses to Protect Against Low and Mid-Tier Threats (DSB report page 9).

The DOD should establish an enterprise security architecture, including appropriate "Building Codes and Standards", that ensure the availability of enabling enterprise missions . . . . The DOD should leverage commercial technologies to automate portions of network maintenance and "real-time" mitigation of detected malware . . . . USD(P&R), in Collaboration with the DOD CIO and the Service Chiefs Establish a Formal Career Path for DOD Civilian and Military Personnel Engaged in Cyber Defense

Examples of ongoing efforts
- Developed JIE enterprise security architecture for unclassified, secret, and coalition networks
- Migrating all internet-facing servers into a separate zone to isolate and contain attacks
- Improving SIPRNET/Coalition/Federal gateways and NIPRNET/Internet boundary defenses
- Developing a Department-wide Cyber Workforce Strategy that includes military and civilian qualifications and career paths
- Automating continuous monitoring of cyber vulnerability via use of the already deployed Host-Based Security System (HBSS)

DSB Recommendation #6: Change DOD's Culture Regarding Cyber and Cyber Security (DSB report page 10). Commander, USCYBERCOM and the DOD CIO establish a plan with measurable milestones and flow down to all organization elements.

Examples of ongoing efforts
- Creating a capstone Cyber Defense strategy document, describing strategic imperatives that will change behavior, culture, operations, and intelligence support (e.g., Defending DOD Networks, Systems, and Data: Strategic Choices for 2020)
- Conducting annual IA training across the DOD
- Simulating "Phish-me" exercises and other real life exercises
- Providing each organization and its chain of command an automated cyber risk score via continuous monitoring

DSB Recommendation #7: Build a Cyber Resilient Force (DSB report page 11). DEPSECDEF should direct specific actions to introduce cyber resiliency requirements throughout DOD force structure.

For programs not part of the segmented force, provide a cyber standard set of requirements (expected to be a subset of the critical program requirements list) to be applied to all DOD programs (USD(AT&L), DOD CIO, SAEs))

Develop DOD-wide cyber technical workforce to support the build out of the cyber critical survivable mission capability and rolled out to DOD force structure (USD(AT&L), CIO, SAEs, DOT&E, USD(I), USD(P&R)).

Examples of ongoing efforts
- DOD CIO and USCYBERCOM identifying key cyber terrain and infrastructure that supports critical C4 systems and assets in order to assure mission execution while under degraded cyber conditions
- Developing Resiliency Framework criteria that helps delineate requirements for contracts and that can be used in the acquisition process
- Creating Cyber security Implementation Guidebook to assist acquisition program managers in successfully implementing cyber security requirements (with AT&L)
- Use of Cyber Ranges for simulated live fire cyber security exercises with active Red Team participation

[See page 9.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 13, 2013

QUESTIONS SUBMITTED BY MR. THORNBERRY

Mr. THORNBERRY. Will you comment on requirements and guidelines being generated by CYBERCOM with respect to an insider threat program? How do you prevent implementation of this policy devolving into a mere "check the box" requirement that does little to enhance our security? The FY13 NDAA included language on next generation host-based security solutions and mentioned insider threat mitigation as one of those capabilities that needed to be addressed in this context. Are CYBERCOM's guidelines going to specify that established host-based solutions are required to satisfy the enterprise monitoring and audit requirements? As a part of your overall risk mitigation strategy, which networks will your requirements cover in terms of Insider Threat Monitoring?

General ALEXANDER. USCYBERCOM has developed requirements for implementation of insider threat capabilities on DOD networks in coordination with the National Insider Threat Task Force (NITTF) and the Comprehensive National Cybersecurity Initiative to develop and implement a government-wide Cyber Counterintelligence Plan (CNCI 6) to achieve the objectives described in the FY13 NDAA. These insider threat requirements include auditing and monitoring, insider threat awareness and training, foreign travel and contact reporting, polygraphs, personnel security, evaluation, analysis, and reporting and security incident reporting and evaluation. This provides a comprehensive defense-in-depth strategy for the detection of and protection from the insider threat. In addition, these capabilities will deter malicious insider activity. The comprehensiveness of this approach prevents the policy from becoming a "check the box" requirement. USCYBERCOM directives as spelled out in OPORD 12–106 specify that host-based solutions are required to satisfy the enterprise monitoring and audit requirements. All U.S. owned and operated DOD Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) networks are covered by these requirements for host-based security and insider threat monitoring.

Mr. THORNBERRY. What progress has DOD made in improving the agility and flexibility of the IT acquisition process?

Ms. MCGRATH. DOD has taken a number of important steps to improve the agility and flexibility of our IT acquisition processes both through policy and through proactive involvement with active IT acquisition programs. A common theme of these efforts has been to tailor the processes to the unique attributes of IT in a way that speeds delivery of capability into the hands of our users.

One important development has been the adoption of an acquisition model tailored for defense business systems. This alternative acquisition model provides a comprehensive process that aligns requirements, investment, and acquisition processes for defense business systems under an integrated governance framework and focuses on incremental delivery of capability, within eighteen months of program initiation. This incremental approach improves control over cost, schedule and performance requirements.

The Under Secretary of Defense (Acquisition, Technology & Logistics) issued implementing policy for this model in the summer of 2011 and the guidance was incorporated into the Defense Acquisition Guidebook in the fall of 2012. This policy is being incorporated into the next update of the DOD 5000.02 acquisition instruction. The Defense Enterprise Accounting and Management System (DEAMS), an Air Force financial management program, was the first program to achieve an acquisition decision under this new policy and we are in the process of transitioning several other major IT programs to this new approach as well.

Through the use of this approach, DEAMS has integrated traditionally stovepiped processes and enabled tight integration between the functional sponsor and the program office. We continue to conduct targeted outreach with Program Managers, Functional Sponsors, and Program Executive Officers on this new policy, and are working with the Defense Acquisition University to embed the new process into appropriate curriculum.

Mr. THORNBERRY. In the FY12 NDAA, this committee directed the establishment of an insider threat detection program. Can you please describe the current status of this effort, which is supposed to achieve full operational capability later this year?

Ms. TAKAI. DOD has been actively participating in National Insider Threat Task Force (NITTF) addressing government-wide insider threat issue—consistent with EO 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." The NITTF issued implementation guidance of EO 13587 via Presidential memo on Nov 21, 2012.

Internally, DOD has:

- instituted read/write controls for external secret computer access ports and restrictions and audits of removable media (USBs, etc.,);
- driven out anonymity and instituted access control through public key infrastructure (PKI) implementation; and
- improved our ability to detect anomalous or malicious behavior on the DOD's secret network.
  - o Provides limited ability to discern data access that signal exceptions to normal data access.
  - o Provides full packet capture in order to discern patterns of malicious activity and allow for the investigation of incidents.

Mr. THORNBERRY. How will the Joint Information Enterprise (JIE) interact with other major IT related initiatives, like the Defense Intelligence Information Enterprise or electronic health records interoperability? Will it be interoperable with the networks of the Intelligence Community?

Ms. TAKAI. The DOD CIO is leading the DOD's IT effectiveness effort to achieve the Joint Information Environment (JIE) and the Director of National Intelligence CIO is leading a similar effort of the Intelligence Community Information Technology Enterprise. Both CIO's share common objectives and end-states, and actively participate on each other's governance boards, standards and architect forums, and Identity Management and data framework forums. Both CIO's recently established a Joint Information Standards Committee (JESC), and a directed policy governing the reuse of standards and specifications between the two communities to ensure interoperability and information sharing.

The Defense Intelligence Information Enterprise (DI2E) is a unifying construct between the Department of Defense, the Intelligence Community (IC), and coalition Intelligence Information Enterprises, and aligns with the Intelligence Community IT Enterprise (ICITE) and DOD Joint Information Enterprise (JIE) policy and strategy.

The DI2E Governance Council oversees development and implementation of a DI2E that is standardized, secure, optimized and interoperable, that aligns with DOD, IC and Coalition IT Enterprises. The Council coordinates on similar efforts by the IC Chief Information Officer (CIO), the DOD CIO, and the Defense Information Systems Agency (DISA) to ensure intelligence information integration across all security domains, including top secret, secret, unclassified, and various coalition fabrics. It enables seamless theater intelligence architectures and achieves efficiencies across the Defense Intelligence enterprise by recommending cost saving measures.

With respect to electronic health records interoperability, DOD is establishing a Medical Community of Interest (Med-COI) virtual network, under the auspices of JIE and its single security architecture. The Med-COI, using the JIE architectural construct, will provide enterprise services and operate within the secure and protected DOD Global Information Grid (GIG). This capability will support unhindered and timely data access of patient records for DOD and VA clinicians and adjudication of VA Benefit claims.

Mr. THORNBERRY. What role does the Cyber Investment Management Board (CIMB) play in decisions related to the JIE, especially with decisions related to service-specific system and network acquisitions?

Ms. TAKAI. The CIMB is an advisory and management body, established to facilitate cohesion across S&T, requirements, acquisition, R&D, T&E, and sustainment efforts to ensure that cyber warfare investments are effectively coordinated across the Department. In this capacity, the CIMB is intended to provide a framework to make resourcing prioritization recommendations consistent with established JIE milestones.

Mr. THORNBERRY. In discussing the Joint Information Environment (JIE), there seems to be a lot that is aspirational with this construct, but you will be limited by the current network environment that you have. How does DOD plan to get from the current "as-is" state to the ideal "to-be" state?

Ms. TAKAI. DOD is continually modernizing its IT infrastructure and systems, and has several "network" initiatives on-going (i.e., LANDWARNET, AFNET, NGEN, etc.) that are focused on achieving the same objectives as JIE for the individual Military Services. JIE effort will leverage their already planned activities and technology refresh cycles to optimize the current network environment to our desired

"to-be" state from an enterprise perspective. At the enterprise level, DISA has planned upgrades of the Defense Information Systems Network (DISN) consistent with the target architecture for the JIE, to include the replacement of circuit-based switches with IP-enabled technologies, and replacement of legacy transport routing to Multiprotocol Label Switching (MPLS). The detailed solution architectures for the JIE are scheduled for completion in June 2013, and are being incorporated into Component programming activities for FY15 and beyond. The Department's JIE Technical Synchronization Office (JTSO) is developing a consolidated synchronization plan in conjunction with other DOD Components.

Mr. THORNBERRY. Last year, the House Oversight and Government Reform committee introduced the Federal Information Technology Acquisition Reform Act (FITARA). Are you familiar with this proposed legislation? If so, what thoughts do you have on how this might affect DOD equities?

Ms. TAKAI. I am aware of the some of the provisions of last year's draft bill, as well as the current version that was introduced earlier this year. I believe because of the complexity of the Department's missions, we will need to examine the legislation carefully to ensure that it does not undo important relationships we have developed between the Office of the Secretary of Defense and the Services and Agencies as well as introduce new or overlapping requirements for the Department for its IT investments.

Mr. THORNBERRY. Following the termination of the Net-Enabled Command Capability (NECC), what is the Department doing to modernize its command and control capabilities?

Ms. TAKAI. The Department is executing a sustainment and modernization plan to evolve the current Global Command and Control System (GCCS) family of systems and related command and control programs to improve mission effectiveness, achieve efficiencies, and provide required command and control capabilities to the joint warfighter. Our sustainment and modernization efforts will ensure support to current operational priorities while migrating to objective capabilities described in the recently updated Joint C2 Capability Development Document (CDD).

Mr. THORNBERRY. How do you plan to address "Bring-Your-Own-Device" (BYOD) policy and the use of cloud technologies? Also, how can DOD keep up with the rate of technological change while using the DFAR? Are current acquisition reform efforts sufficient?

Ms. TAKAI. Bring Your Own Device (BYOD) and portable cloud services are emerging trends in commercial industry. Many issues must be addressed before the DOD can embrace these technologies, such as overcoming existing DOD policy constraints, understanding the various operational use scenarios, examining potential security vulnerabilities, and avoiding potential legal issues that surround BYOD solutions. My office published the DOD Mobile Device Strategy on June 8, 2012, and the DOD Commercial Mobile Device Implementation Plan on February 15, 2013, with the focus on improving three areas that are critical to mobility: 1) the networking infrastructure to support wireless mobile devices, 2) mobile applications, and 3) a framework that will allow the Department to sustain a commercial mobile solution that is reliable, secure, and flexible enough to keep pace with fast-changing technology. The DOD CIO will continue to monitor BYOD efforts across our Federal Government and, in conjunction with the Digital Government Strategy, will continue to evaluate BYOD options.

Cloud Computing is becoming a critical component of the Joint Information Environment (JIE) and the Department's Information Technology (IT) modernization efforts and will enable users the access to data anywhere, anytime on any approved device. One key objective is to drive the delivery and adoption of a secure, dependable, resilient multi-provider enterprise cloud computing environment that will enhance mission effectiveness and improve IT efficiencies. Cloud services will enhance warfighter mobility by providing secure access to mission data and enterprise services regardless of where the user is located and what device he or she uses.

My office recently issued the DOD Cloud Computing Strategy to provide an approach to move the Department to an end state that is an agile, secure, and cost effective service environment that can rapidly respond to changing mission needs. There are two key components of the Department's cloud strategy. The first component is the establishment of a private enterprise cloud infrastructure that supports the full range of DOD activities in unclassified and classified environments and optimizes data center consolidation efforts. The second is the Department's adoption of commercial cloud services that can meet the Department's cybersecurity and other IT needs while providing capabilities that are at least as effective and efficient as those provided internally.

The Defense Information Systems Agency (DISA) is designated the DOD Enterprise Cloud Service Broker to facilitate and optimize access and use of commercial

cloud services that can meet DOD's security and interoperability requirements, and ensure that new services are not duplicative of others within the Department while consolidating cloud service demand at an enterprise level. In addition, DISA, as the DOD broker, will leverage the Federal Risk Authorization and Management Program (FedRAMP) standardized security authorization process, including the accepted minimum security baseline for low and moderate information security categorizations, and ongoing continuous monitoring to ensure that appropriate security controls remain in place and are functioning properly.

Current acquisition reform efforts offer opportunities to accelerate the adoption of commercial technologies. In many respects, despite their rapid evolution, mobility solutions are much like other traditional IT systems that empower users and managers with the tools and information they need to execute their missions. Our strategy of integrating well-orchestrated limited deployment pilot implementations allows users and managers to rapidly innovate, mature critical technologies, and resolve integration challenges to swiftly address mission challenges. The Implementation Plan incorporates many of the Services technology development efforts in a spiral approach with an 18-month acquisition cycle. The Implementation Plan streamlines the certification and accreditation (C&A) process for mobile devices, operating systems, and applications. Sharing the workload with industry will bring the timeline for C&A down from over 18 months to about 30 days with no reduction in security posture. Though the platforms will continue to evolve, we have the same commitment to systematic acquisition practices that serve the defense community most effectively. We continue to review the mobility acquisition lifecycle for efficiency opportunities.

Mr. THORNBERRY. Would you tell us how much funding has been set aside to assist DOD organizations in establishing Insider Threat Programs in accordance with the recent Presidential Mandate, Memo, and National Insider Threat Standards? Further, who will be the organization responsible for identifying and distributing the necessary funding to each DOD entity? Who will be on point from your office to ensure the funding is being appropriately spent on the Insider Threat Mission within each DOD entity? Are there additional monies coming from the ODNI or the Office of the National Counterintelligence Executive (NCIX) for Enterprise Audit and Insider Threat missions?

Ms. TAKAI. The Department initially programmed $162M, FY12–16, in order to satisfy the Executive Order 13587 requirements. The Department is assessing the need for additional resources to address the insider threat as part of our FY 15 budget deliberations. The Defense Information Systems Agency (DISA) and the Defense Manpower Data Center (DMDC) are the responsible implementing agencies for the initial $162M. My office is overseeing implementation of the budgeted and programmed funds provided to date. The Department is developing the necessary policy and responsibilities required under the Presidential mandate issued November 21, 2012. Regarding additional monies, there has been limited funding provided to a number of our Title 50 elements by ODNI and NCIX in FY 11 and 12. We don't anticipate any additional funding from ODNI or NCIX.

Mr. THORNBERRY. Does the Department have a strategy to leverage commercial cyber security solutions to enable it to benefit from such capabilities as real time, global threat intelligence that has been optimized to work in highly sensitive environments? Who in the Department is responsible for the operational requirements, technical requirements, funding and acquisition? When does the Department plan to start executing against each of these requirements?

Ms. TAKAI. Yes, for instance, initial funding was secured beginning in FY 14, under the program name "Zero day Network Defense" (ZND) which consists of commercial tools to be acquired and deployed in partnership between the Defense Information Systems Agency (DISA) and NSA to provide this defensive capability at the DOD perimeter, and on classified end point systems.

While unclassified systems are just beginning to use this technology from commercial vendors, we are currently seeking funding to expand the ZND capability to unclassified networks and develop a Global Reputation Service that will be capable of ingesting information from commercial vendors, as well as government sources.

The requirements for this capability were derived from multiple sources, including the Cyber Situational Awareness Initial Capabilities Document with input from all DOD components and agencies.

QUESTIONS SUBMITTED BY MR. LANGEVIN

Mr. LANGEVIN. General Alexander, in testimony before the Senate Armed Services Committee on Tuesday, you noted the creation of 13 teams with an offensive focus.

Given that cyber in many cases requires preparatory work in order to access the full range of capabilities, how forward-leaning will these teams be?

What training will you be providing to the identified mission teams and to other personnel who are being assigned to cyber work? Do you require additional authorities or resources in order to fully train the men and women under your command, particularly with regard to language skills, emulation and red-teaming?

General ALEXANDER. USCYBERCOM identified 42 specific work roles and the standards and skills required for planning and executing cyberspace operations. We worked with the National Security Agency, Service Departments, academia, and the private sector to leverage existing training solutions and created new ones, as appropriate, to train the personnel assigned to those work roles (see Exhibit A for additional detail.) Over the next three years we will train the Cyber Mission Forces that will perform world-class offensive and defensive cyber operations as part of our Cyber National Mission Teams, Cyber Combat Mission Teams and Cyber Protection Forces. We do not require additional authorities or resources to train the currently identified cyber professionals.

[Exhibit A is For Official Use Only and is retained in the committee files.]

Mr. LANGEVIN. Ms. Takai, what progress has DOD made in improving the agility and flexibility of the IT acquisition process, and is there additional Congressional action needed?

Ms. TAKAI. There are unique characteristics associated with the acquisition of information systems that require the use of acquisition approaches different from those normally used by the Department for acquiring weapons systems. All acquisition approaches should be tailored to the nature of the product being acquired. For example, information systems (e.g. business systems) do not require significant technology development like many weapons systems and they do not have the long term operations and support challenges facing most weapons systems. The Department has made steady progress in implementing several of the key approaches for improving the agility and flexibility of the IT acquisition process in the areas of requirements, acquisition, testing and certification and human capital. Many of these efforts will be captured in the next release of DODI 5000.02, "Operation of the Defense Acquisition System" including:

- Requirements: The Joint Staff has updated the requirements management process (Joint Capability Integration and Development System (JCIDS) to include a more streamlined requirements management and approval process for acquisition of information systems.
- Acquisition: On June 23, 2011, a Directive-Type Memorandum (DTM) on Business Capability Lifecycle (BCL) was signed and issued by USD (AT&L). The BCL provides a framework for implementing more flexible and streamlined processes for the acquisition of these business information systems and has been incorporated into the next release of DOD 5000.2.
- Test and Certification: The Department's testing community has been working in collaboration with USD (AT&L) to incorporate an integrated testing, evaluation, and certification approach into the DODI 5000.02, to reduce redundancies in system testing activities and improve the efficiency and effectiveness of testing the Department's information systems.
- Human Capital: A comprehensive review of IT acquisition competencies is also currently being conducted by the Department's Chief Information Officer. This review will update the IT acquisition competencies to better define DOD critical skill sets and assist in the update of curricula at the Defense Acquisition University and the Information Resources Management College.

QUESTIONS SUBMITTED BY MR. ROGERS

Mr. ROGERS. Ms. Takai, could you please explain the Department's decision-making process for when to use "sole source" and "brand name only" solicitations, such as those run under the Air Force's NETCENTS–1 and NETCENTS–2 contracts?

Ms. TAKAI. The vast majority of procurements through the NETCENTS vehicles are accomplished via a competitive process. In the rare event that a sole source or specific brand name is required, appropriate Justification and Approval documentation is prepared and approved at a level commensurate with the dollar value of the proposed procurement.

Mr. ROGERS. What steps does DOD take to meet the statutory requirements of FAR sec. 6.303 and/or FAR sec. 16.505, as applicable, that are the prerequisites for a sole source and/or brand name product procurement, single name product procure-

ment, including the necessity to conduct open procurements, determine minimum needs, and solicit the interest of manufacturers or prospective offerors?

Ms. TAKAI. All DOD requiring officials must follow and adhere to applicable procurement policies in accordance with the Defense Federal Acquisition Regulation Supplement (DFARS), which is regularly revised to ensure alignment with the Federal Acquisition Regulations (FAR) as well as other regulations and statutes. DFARS subpart 216.5 requires that all orders for supplies or services exceeding $150,000 that are placed under multiple award contracts be awarded on a competitive basis with fair notice given to vendors of the intent to purchase, and an opportunity for all vendors to submit offers and receive fair consideration. There are allowable exceptions that must be based on justifications and/or determinations written and approved in accordance with FAR 8.405–6; if a statute requires the purchase be made from a particular source, or if one of the circumstances described in FAR 16.505 (b) (2) (i) through (iv) applies. DOD contracting officers must always consider price or cost as factors when selecting a vendor for award, and should also consider past performance of potential vendors. As an overview, the steps followed to award in DOD include: 1) system engineering analysis to determine requirements, 2) market research to determine what products are available to satisfy those requirements, and 3) written documentation via a determination or Justification and Approval of anything less than full and open competition (including specification of a particular brand name product). Even when a particular brand name product is required and justified, there is an expectation of competition if there are multiple competing resellers of that same brand name product.

Mr. ROGERS. When the requirements of FAR sec. 6.303 and/or FAR sec. 16.505, as applicable, are determined not to have been met, what remedial steps are in place to make sure these requirements are considered?

Ms. TAKAI. There are many stages at which such a determination might be made, such as: by the program manager after market research activities, by the contracting officer or the contracting activity's Competition Advocate prior to solicitation and/or award or by the Government Accountability Office after an unsuccessful vendor files an appeal. There are different remedial steps for each scenario. Standard DOD acquisition and procurement procedures contain safeguards and checkpoints at multiple levels to ensure that any proposed exceptions to the competition rules are fully vetted and adequately justified. DOD contracting officers must make public the justification(s) required by FAR 6.303–1 in accordance with FAR 5.3 and as required by law. If a prospective (or unsuccessful) offeror believes that the procedures described in the FAR and/or DFARS have not been followed, they will generally contact the contracting officer who has responsibility for the acquisition, or the contracting activity's parent organization. If warranted, the contracting officer can then cancel the procurement activity—or issue a "stop work" order to study the situation (if the contract has already been awarded). In order to meet the requirements of the requesting office, the contracting officer may reshape the procurement into a competition among multiple vendors under a pre-existing contract vehicle, or pursue full and open competition among all vendors of a particular type/class of capability.

Mr. ROGERS. What process does DOD use in deciding to standardize on particular technology, and how does such standardization further the goal of maintaining a competitive procurement process which is essential to reducing costs in government procurements? Does that process flow down to how the Services make similar decisions?

Ms. TAKAI. When there are clearly definable minimum functional/technical standards that are available and necessary to attain a required capability, the DOD CIO will assemble a cross-Component "tiger team" (including Acquisition personnel) to translate those standards into requirements suitable for release of an Request for Quotes (RFQ) or a Request for Proposals (RFP) to industry. For example, when data-at-rest (DAR) software was initially identified as an urgent requirement for all DOD laptops and portable computers, the Defense-Wide Information Assurance Program (DIAP) assembled such a tiger team to flesh out the applicable required specifications. Then they partnered with the DOD ESI Software Product Manager team from USAF to translate these specifications into an industry solicitation that resulted in the creation of DOD ESI Blanket Purchase Agreements from 10 different publishers of DAR software. By DOD CIO policy, all DOD buyers of DAR software were required to buy DAR software only through one of these agreements. Competition among the resellers generally resulted in lower prices, and the DIAP certified that all purchased products met both the functional & technical standards.

QUESTIONS SUBMITTED BY MR. FRANKS

Mr. FRANKS. General Alexander, I want to thank you for your service and leading such important missions with USCYBERCOM and the NSA. I am a strong believer that our military is, and should always be, better than the rest of the world's armed forces, and that we should never be entering fair fights. With that in mind, and the introduction of these new offensive cyber teams, and the fact that cyber threats are a relatively new phenomenon, how much better are we on offense, and defense in the cyber realm as compared to our enemies.

General ALEXANDER. We believe our offense is the best in the world. Cyber offense requires a deep, persistent and pervasive presence on adversary networks in order to precisely deliver effects. We maintain that access, gain deep understanding of the adversary, and develop offensive capabilities through the advanced skills and tradecraft of our analysts, operators and developers. When authorized to deliver offensive cyber effects, our technological and operational superiority delivers unparalleled effects against our adversaries systems.

Team Cyber is constantly increasing its operational and analytic defensive capabilities through the adoption and use of standards to facilitate domain knowledge representation and information sharing across the community. In addition, the use of standards ensures compatibility with technologies commonly available in the public domain and allows for the rapid integration of new functional capabilities to avoid long-term engineering and development cycles.

Potential adversaries are demonstrating a rapidly increasing level of sophistication in their offensive cyber capabilities and tactics. In order for the Department of Defense to deny these adversaries an asymmetric advantage, it is essential that we continue the rapid development and resourcing of our Cyber Mission Forces.

Mr. FRANKS. General Alexander, last year I asked you a question: How prepared are we to carry out your mission if the power grid or substantial part of it were to go down for an extended period of time? For example, two weeks or longer due to severe space weather or a manmade electromagnetic pulse.

Your answer included that fact that much of DOD's cyberspace is served through commercial providers. Do you feel that the power and electricity needed to carry out your mission is important enough to require those commercial providers of the power grid to successfully harden their grid from severe space weather or manmade electromagnetic pulse? Can the DOD require that of commercial providers of the grid? Do you feel that this issue is important enough that legislation is needed to force the hand of industry to act?

General ALEXANDER. While I absolutely agree with the criticality of cyber hardening the power grid, I also believe any legislative solution has to take into account the prohibitive costs associated with doing so given its antiquated state. I believe the activities underway through the President's EO 13636 "Improving Critical Infrastructure Cybersecurity" and PPD–21 "Critical Infrastructure Security and Resilience" are a good first step. Legislation which builds upon these activities by providing the right set of incentives would be invaluable.

From an NSA and CYBERCOM perspective, it is also critical that Congress pass information sharing legislation that enables effective two-way sharing of cyber threat information and countermeasures between the private sector and the USG. By effective two-way sharing, I mean that the government needs to know, in real time, when there are indications of cyber intrusions or attacks against the nation's critical infrastructure, and the government needs to be able to share in real time, indications and warnings of attacks and associated countermeasures that the private sector needs to protect their networks. Given the authority to share information, the ISPs could act as a domestic radar that can see cyber threats and tip and queue the government to respond in real time.