S. HRG. 113–611

NOMINATIONS BEFORE THE SENATE ARMED SERVICES COMMITTEE, SECOND SESSION, 113TH CONGRESS

HEARINGS

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

ON

NOMINATIONS OF

HON. MADELYN R. CREEDON; HON. BRAD R. CARSON; DR. WILLIAM A. LaPLANTE, JR.; HON. ROBERT O. WORK; HON. MICHAEL J. McCORD; MS. CHRISTINE E. WORMUTH; MR. BRIAN P. McKEON; HON. DAVID B. SHEAR; MR. ERIC ROSENBACH; GEN. PAUL J. SELVA, USAF; VADM MICHAEL S. ROGERS, USN; DR. LAURA J. JUNOR; MR. GORDON O. TANNER; MS. DEBRA S. WADA; MS. MIRANDA A.A. BALLENTINE; DR. MONICA C. REGALBUTO; ADM WILLIAM E. GORTNEY, USN; GEN JOHN F. CAMPBELL, USA; LTG JOSEPH L. VOTEL, USA; GEN. JOSEPH F. DUNFORD, JR., USMC; MR. ROBERT M. SCHER; MS. ELISSA SLOTKIN; MR. DAVID J. BERTEAU; MS. ALISSA M. STARZAK; AND ADM HARRY B. HARRIS, JR., USN

JANUARY 16; FEBRUARY 25; MARCH 11; JUNE 19; JULY 10, 17; DECEMBER 2, 2014

Printed for the use of the Committee on Armed Services

NOMINATIONS OF GEN. PAUL J. SELVA, USAF, FOR REAPPOINTMENT TO THE GRADE OF GENERAL AND TO BE COMMANDER, U.S. TRANSPORTATION COMMAND; AND VADM MICHAEL S. ROGERS, USN, TO BE ADMIRAL AND DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICES/COMMANDER, U.S. CYBER COMMAND

TUESDAY, MARCH 11, 2014

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

The committee met, pursuant to notice, at 9:37 a.m. in room SD–G50, Dirksen Senate Office Building, Senator Carl Levin (chairman) presiding.

Committee members present: Senators Levin, Reed, Udall, Manchin, Blumenthal, Donnelly, Kaine, King, Inhofe, McCain, Chambliss, Wicker, Ayotte, Graham, Vitter, Lee, and Cruz.

Other Senator present: Senator Kirk.

OPENING STATEMENT OF SENATOR CARL LEVIN, CHAIRMAN

Chairman LEVIN. Good morning, everybody. The committee meets today to consider the nomination of General Paul Selva to be Commander of the U.S. Transportation Command (TRANSCOM); Admiral Michael Rogers to be Commander, U.S. Cyber Command (CYBERCOM), Director of the National Security Agency (NSA), and Director of the Central Security Service.

We welcome our nominees. We thank you for your many years of service and for your willingness to continue to serve in positions of great responsibility, and of course we thank your families, who give up so much to enable you to serve.

TRANSCOM, which encompasses the Air Force's Mobility Command, the Navy's Military Sealift Command, the Army's Surface Deployment and Distribution Command, is the linchpin of our strategic mobility. TRANSCOM has played a crucial role in supplying our operations in Iraq and Afghanistan. It has also taken the lead in bringing troops and equipment home from Afghanistan.

We'd be interested in the nominee's views on how long we can wait for a bilateral security agreement to be signed by President Karzai or his successor and still meet the December 31, 2014, deadline for removing all of our people and equipment from Afghanistan

in the event—and I emphasize—in the event we end up without an agreement.

Like other elements of the Department of Defense (DOD), TRANSCOM suffers from constant threats from cyber intrusions. Because of the command's reliance on the commercial sector to supplement its transportation capacity, it must be sensitive not only to the vulnerability of its own computer systems, but also to the vulnerability of the private companies that it relies on to mobilize, transport, and resupply our troops.

Our committee will soon release a report on cyber intrusions affecting TRANSCOM contractors and the extent to which information about such intrusion reaches TRANSCOM and other key entities within DOD. That's an issue which touches both of the nominees' prospective commands. We welcome your thoughts on dealing with this ongoing problem.

Last month, we heard testimony from General Alexander, the current CYBERCOM Commander, regarding a number of pressing issues currently facing the command. We look forward to hearing Admiral Rogers' views on many of the same issues, including the qualifications of the personnel that the Military Services are making available for their new cyber units, the tools and data sources these forces will have to work with, the ability of the Military Services to manage the careers of their growing cadre of cyber specialists, and the steps that should be taken to ensure that the Reserve components are effectively integrated into the cyber mission.

The committee will also be interested in Admiral Rogers' views on the collection of bulk telephone call records, the collection of the contents of Internet communications, and other NSA programs that have raised public concerns about threats to privacy and to civil liberties. For example, Admiral, we would like to know your reaction to the recent statement of the Privacy and Civil Liberties Oversight Board with respect to the section 215 telephone call record program that they have not, and this is the board saying this, that they have not, "identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation."

We'd be interested in knowing what steps, Admiral, you would take if confirmed to assess the continuing value of this program and to weigh that value against its potential impact on privacy and civil liberties. Do you support the President's recent directive to modify the program so that bulk records are no longer held by the Government, while ensuring that these records can be accessed when necessary? What is your view on the threshold or standard that the Government should be required to meet to search through such data? Admiral Rogers will play a key role in providing advice on these and other issues.

Thanks again to both of our nominees for being here today, for your service to the Nation over many, many years, and your willingness to continue that service.

Senator Inhofe.

Senator INHOFE. Thank you, Mr. Chairman.

Two weeks ago I expressed to General Alexander my support for the progress under way at CYBERCOM to normalize cyber planning and capabilities. Despite these critical strides, the lack of a

cyber-deterrence policy and the failure to establish meaningful norms that punish bad behavior have left us more vulnerable to continued cyber aggression. In particular, I'm deeply concerned about the two well-publicized events by Iran that involved an enduring campaign of cyber-attacks on U.S. banks and the financial sector and another involving the exploitation of a critical Navy network.

The administration's failure to acknowledge or establish penalties for these actions emboldens countries like North Korea, Russia, China, and places American infrastructure such as the power grid or Wall Street at greater risk. The President's going to have to get serious and develop a meaningful cyber deterrence policy.

General Selva, TRANSCOM provides the lifeline for every other combatant command by enabling them to execute a wide array of missions from combat operations to humanitarian relief, from training exercises to supporting coalition partners. I'm interested in your assessment of the readiness of TRANSCOM and its components, including the viability of the commercial sector to support TRANSCOM missions. I'm also interested in your assessment of TRANSCOM's ability to meet U.S. Central Command (CENTCOM) and International Security Assistance Force (ISAF) requirements.

General Fraser testified last year that the number of cyber-attacks against TRANSCOM had doubled from 45,000 in 2011 to nearly 100,000 in 2012. The committee has been investigating these incidents and it appears that there are a number of factors that should be addressed to ensure that TRANSCOM has the information necessary from its many contractors to defend its networks and protect mission-critical data.

I look forward to hearing from our nominees on how they intend to work together to ensure that these issues are corrected and TRANSCOM's classified and unclassified networks are secured. It's something that not many people know about, but I don't draw a distinction between a cyber-attack and a military attack in places. We'll have a chance to talk about that during the questioning.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator Inhofe.

We're delighted to have Senator Kirk with us this morning to introduce one of our nominees. It's great to have you with this committee and to call on you now for your introduction.

STATEMENT OF HON. MARK KIRK, U.S. SENATOR FROM THE STATE OF ILLINOIS

Senator KIRK. Thank you, Mr. Chairman. Mr. Chairman, I'm here to introduce Mike Rogers to the committee. I have known Mike Rogers for almost 40 years. We were in the same home room in high school together. I had the honor to work for Mike as a reservist when he was the head of intel for the Joint Chiefs of Staff.

I would say that you cannot pick a better guy, an officer who has a stronger work ethic or detail orientation, than Mike. I wanted to say that being a Republican, I have not supported a lot of the nominees of the President. I would say that this is the best American you could have picked for this job.

That would conclude my statement.

Chairman LEVIN. Thank you so much for that wonderful introduction.

The first question we're going to ask Admiral Rogers is what did he know about you in home room. He's going to tell us some secrets that you have now unleashed on yourself, I think.

Thank you for being with us, Senator Kirk.

All right. We'll call on, I think in order of their being listed, General Selva. Of course, Senator Kirk, you're free to stay or leave because we know you have a tough schedule. General Selva.

STATEMENT OF GEN. PAUL J. SELVA, USAF, FOR REAPPOINTMENT TO THE GRADE OF GENERAL AND TO BE COMMANDER, U.S. TRANSPORTATION COMMAND

General SELVA. Chairman Levin, Senator Inhofe, distinguished members of the Senate Armed Services Committee, it's a great honor to appear before you today as the President's nominee to be the Commander of U.S. Transportation Command. First I want to thank the members of this committee for their steadfast support of the airmen in Air Mobility Command, who throughout the last decade have literally moved mountains to support our soldiers, sailors, airmen, and marines in Iraq and Afghanistan. It's because of your continued support that they've been able to provide the global reach that's so important to this great Nation.

If confirmed, I look forward to working with you and other relevant committees to navigate the challenges of leading the men and women of TRANSCOM.

I'm proud today to introduce you to my wife Ricky, who's seated right behind me, who has served with me and by my side for our 34 years of marriage, since our graduation as classmates from the U.S. Air Force Academy. She served in uniform for 9 years and gives generously of her time now to support the amazing airmen and their families that are part of Air Mobility Command. She is the love of my life and, apart from my mother, is one of the very few people that can give me the unabashed feedback I need when I step away from centerline.

It's also a privilege to be here today with a friend and colleague, Admiral Mike Rogers, with whom I have served on the Joint Staff, and I can think of no better person to serve in the capacity for which he has been nominated.

If confirmed, I look forward to working with the soldiers, sailors, airmen, and marines of TRANSCOM, Active, Guard, Reserve, and their civilian counterparts, as well as the vast network of commercial partners that provide the distribution and logistics networks that make our Nation successful.

I appreciate the trust and confidence that the President, Secretary of Defense, and General Dempsey have put in me in considering me for this position. I'm grateful for the opportunity to be before you here today and I look forward to your questions. Thank you, Mr. Chairman.

Chairman LEVIN. General, thank you so much. Again, I'm glad you introduced your family. I should have indicated that you're both welcome to introduce family and anyone else who's here to support you. We're delighted you did that.

Admiral.

STATEMENT OF VADM MICHAEL S. ROGERS, USN, TO BE ADMIRAL AND DIRECTOR, NATIONAL SECURITY AGENCY; CHIEF, CENTRAL SECURITY SERVICES; AND COMMANDER, U.S. CYBER COMMAND

Admiral ROGERS. Chairman Levin, Ranking Member Inhofe, and distinguished members of the committee, thank you for the opportunity to appear before you today. I am honored and humbled that the President has nominated me for duty as Commander, U.S. Cyber Command, and designated me as the next Director of the National Security Agency. I also thank Secretary of Defense Hagel and Chairman of the Joint Chiefs of Staff General Dempsey for their confidence in my ability to assume these significant duties.

I'm joined today by my wife, Dana. One evening 30 years ago, in fact here in Washington, DC, she took a chance on a then-young Lieutenant Junior Grade Rogers, which just goes to show that truly great things can happen to a sailor on liberty. I want to very publicly thank her for her love and support, both for the past nearly 29 years of marriage and for her service to the Nation and, perhaps most importantly, her willingness to take on an even greater set of challenges if I am confirmed.

I have always believed that the life we lead in uniform is even more difficult for our spouses and our families than it is on us, and I am blessed to have a great partner in Dana.

Not with us today are our two sons, Justin, a serving naval officer currently on sea duty, which on a day like today sure sounds like a great place to be, and Patrick, a very hard-working college student.

I'm also honored to be here today alongside General Paul Selva, who, as he has indicated, we have had the pleasure of working together before and I can attest to his significant abilities firsthand.

If confirmed, I look forward to working closely with the members of this committee in addressing the significant cyber challenges facing our Nation today and into the future. We face a growing array of cyber threats from foreign intelligence services, terrorists, criminal groups, and hacktivists, who are increasing their capability to steal, manipulate, or destroy information and networks in a manner that risks compromising our personal and national security. They do so via a manmade environment that is constantly evolving and through the use of techniques and capabilities that are continually changing.

This is hard work and it requires change, something seldom easy either for individuals or for organizations. If confirmed as the Commander, CYBERCOM, my priority will be to generate the capabilities and capacities needed to operate in this dynamic environment and to provide senior decision makers and my fellow operational commanders with a full range of options within the cyber arena. I will partner aggressively with others in doing so, particularly with our allies and partners, those in the private and academic sectors, within DOD and agencies and organizations across the U.S. Government as well as Congress.

I am also mindful that CYBERCOM and the NSA are two different organizations, each having its own identity, authorities, and oversight mechanisms, while executing often related and linked mission sets. Each has the potential to make the other stronger in

executing those missions and I will work to ensure each is appropriately focused. When there is differing opinion between them, I will make the call as the commander, always mindful that the mission of each is to deliver better mission outcomes.

I will also be ever mindful that we must do all of this in a manner which protects the civil liberties and privacy of our citizens. I will ensure strict adherence to policy, law, and the oversight mechanisms in place. I will be an active partner in implementing the changes directed by the President with respect to aspects of the NSA mission, and my intent is to be as transparent as possible in doing so and in the broader execution of my duties if confirmed.

To the men and women of the NSA and CYBERCOM, I thank you for your commitment to the security of our Nation and for your professionalism. I believe in you and in the missions you execute in defending the security of the Nation and its citizens. I am honored to even be considered for duty as your leader and, if confirmed, I look forward to joining the team.

I also want to thank General Keith Alexander for his almost 40 years of commissioned service to this Nation. He has laid a solid foundation at CYBERCOM and the NSA for those who come behind him. He has made a huge contribution in this mission set and I thank him and Debby for all that they have given the Nation.

Finally, let me conclude by thanking those men and women, far too numerous to name individually, who have given me the love and support in my life to live the dream I have had since I was literally a young boy of being a serving naval officer. From those who shaped me in my youth to those who have led, mentored, guided, taught, or in some instances flat-out just kicked me in the tail in my time in uniform when I needed it most, I thank them. I fully realize that I am in no small part here today because of the efforts of so many others in my life.

Thank you again for the opportunity to appear before you and I look forward to answering your questions.

Chairman LEVIN. Admiral, thank you so much.

We have standard questions that we ask of our nominees and here they are: Have you both adhered to applicable laws and regulations governing conflicts of interest?

Admiral ROGERS. I have.

General SELVA. Yes, sir.

Chairman LEVIN. Do you agree, when asked, to give your personal views, even if those views differ from the administration in power?

General SELVA. Yes, sir.

Admiral ROGERS. Yes, sir.

Chairman LEVIN. Have you assumed any duties or undertaken any actions which would appear to presume the outcome of the confirmation process?

Admiral ROGERS. No, sir.

General SELVA. No, sir.

Chairman LEVIN. Will you make sure your staff complies with deadlines established for requested communications, including questions for the record in hearings?

General SELVA. Yes, sir.

Admiral ROGERS. Yes, sir.

Chairman LEVIN. Will you cooperate in providing witnesses and briefers in response to congressional requests?

Admiral ROGERS. Yes, sir.

General SELVA. Yes, sir.

Chairman LEVIN. Will those witnesses be protected from reprisal for their testimony or briefings?

Admiral ROGERS. Yes, sir.

General SELVA. Yes, sir.

Chairman LEVIN. Do you agree, if confirmed, to appear and testify before this committee?

Admiral ROGERS. Yes, sir.

General SELVA. Yes, sir.

Chairman LEVIN. Finally, do you agree to provide documents, including copies of electronic forms of communication, in a timely manner when requested by a duly constituted committee, or to consult with the committee regarding the basis for any good faith delay or denial in providing such documents?

General SELVA. Yes, sir.

Admiral ROGERS. Yes, sir.

Chairman LEVIN. Thank you both.

Let's try 7 minutes for our first round of questions.

General, let me start with you. I asked this in my opening statement, asked you to consider this question: How long can the negotiations on a bilateral security agreement continue before TRANSCOM will be at risk of being able to get all of our cargo out of Afghanistan if there is no bilateral security agreement and we have to leave Afghanistan completely by the end of the year?

General SELVA. Senator, my understanding from consulting with the TRANSCOM staff on that question is that through the early fall we still have sufficient capacity in the variety of networks that we're using to redeploy cargo from Afghanistan to be able to make the decision at that point. To be able to give you a specific date, I'd have to consult with General Lloyd Austin down at CENTCOM, and if confirmed we'll be happy to do so and come back to you with a more definitive answer.

Chairman LEVIN. Thank you.

The next question for you, General, has to do with the intrusions, the cyber intrusions, and whether or not they affect DOD information. Is it not important that TRANSCOM know of cyber intrusions that can pose a risk to operations even if they don't immediately affect DOD data?

General SELVA. Yes, sir. As you're aware, the network that we use inside TRANSCOM consists significantly of our relationship with commercial transportation and logistics providers. Roughly 90 percent of the information in my current position as Air Mobility Command, and I suspect inside TRANSCOM as well, travels across unclassified networks. Being able to maintain the security of those networks through appropriate mechanisms inside those commercial companies is critical to our success.

We have an obligation to be able to assure the validity and veracity of the information that we pass on those networks. As a result, one of the initiatives that's been taken is to include in all of our commercial contracts a stipulation that commercial providers provide us with information on any intrusions into their networks.

I'm not aware of the details of the report that you spoke about, but I look forward to working with your staff on being able to work those details if confirmed.

Chairman LEVIN. Thank you.

Admiral, in January the President ordered a transition to end the section 215 telephone metadata collection program as it currently exists, to, "preserve the capabilities that we need," but without the Government collecting and holding the data on call detail records. Let me ask you this, what in your view are the essential capabilities that need to be preserved in transitioning the program as the President directed? What are those essential capabilities?

Admiral ROGERS. Sir, there's a process ongoing to work through that. I'm not part of that process, but one of my thoughts in particular would be the idea of speed, the ability to query the data, to work with the new mechanisms that we will put in place, and to do so in a timely manner to generate information and insight in a way that enables us to act in a timely manner.

Chairman LEVIN. Now, do you agree that the Government itself does not need to hold all the metadata records in order to determine whether terrorist suspects overseas are communicating with persons located in the United States? In other words, is it possible that a third party could be designated to hold the data on the one hand and then have the service providers keep the data on the other hand?

Admiral ROGERS. I believe, sir, with the right construct we can make that work.

Chairman LEVIN. You could have a third party other than the service providers, or would it be limited to the service providers holding that data?

Admiral ROGERS. Again, I think those are options all under consideration. I believe we could make either scenario work, whether the service providers did it or a third party did it. There are definitely some challenges we'll need to work through, but I'm confident in our ability to do so.

Chairman LEVIN. As I mentioned in my opening statement, the Privacy and Civil Liberties Oversight Board and the President's Review Group on Intelligence and Communications Technology characterized the section 215 program as useful but not critical. The Oversight Board said that, "We have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation."

First of all, do you have an assessment of the utility of the program, and how that utility compares to the level of concern that the American people have about its perceived impact on privacy?

Admiral ROGERS. Sir, first, as the nominee I'm not in a position to really yet be able to comment on the value of 215. But if confirmed I certainly intend to be able to do so. I believe one of the most important functions of the Director of the NSA is to be able to articulate just that, what is the value of our efforts, so that we can make well-informed and smart decisions.

Chairman LEVIN. Do you have an opinion as to whether or not there has been an instance involving a threat to the United States

in which the 215 program made a concrete difference? Do you have an opinion going in on that subject?

Admiral ROGERS. Sir, nothing specific. I have not had a chance to sit down and particularly review the events, although if my memory is correct General Alexander has testified before this committee last month, as you indicated, in which he outlined a number of instances in which he thought 215 generated value.

Chairman LEVIN. This is also for you, Admiral. Do you think DOD is doing enough to provide capabilities for our defensive cyber units by exploiting commercial technology?

Admiral ROGERS. I will use my own experience right now as the Navy component, if you will, to CYBERCOM, where we have a continual outreach to the broader commercial and industry sectors in an attempt to identify just what technologies are available that we could use in the missions. There is an aggressive effort to do so.

Chairman LEVIN. Thank you. Thank you both.

Senator Inhofe.

Senator INHOFE. Thank you, Mr. Chairman.

We've expressed many times our concern about Iran and the threat that they pose to us and that our intelligence, unclassified intelligence, as far back as 2007 indicated that they would have a capability of a weapon and a delivery system by 2015. Then it was even more forcefully expressed in a report that was unclassified by our intelligence in 2010 reaffirming their suspicions earlier.

I've been concerned about that for a long period of time. I'm concerned that we have a President that somehow thinks that there is an opportunity to get them to join the global community and reform their ways. A recent Wall Street Journal article suggested that the Iranians were able to successfully infiltrate the critical Navy computer network. The February 17 article raises serious questions, suggesting Iran was able to access the bloodstream of the Navy network. Now, I'm going to quote from that report:

"Iran's infiltration of a Navy computer network was far more extensive than previously thought. It took the Navy about 4 months to finally purge the hackers from its biggest unclassified computer network."

Now, if that's true, the geopolitical consequences of such an attack should really be profound. However, it remains unclear what, if anything, this administration would do in response to such behavior. Would a similar penetration by the Iranians' warplanes into American air space be treated with such ambivalence? I would hope not.

Admiral Rogers, your current job as Commander of the Fleet Cyber Command means that you are the one responsible for defending Navy networks. This happened on your watch, correct?

Admiral ROGERS. Yes, sir, it did.

Senator INHOFE. What are the consequences of Iranian action in cyber space?

Admiral ROGERS. First, sir, as a matter of policy and for operational security reasons we have never categorized who exactly, publicly, penetrated the network. I would be glad to discuss this with you in a classified session.

Senator INHOFE. No, this has been discussed in an unclassified session for quite some time, that we're talking about Iran in this case. So go ahead.

Admiral ROGERS. I'm sorry, sir. Not to my knowledge. I apologize.

Specifically, a segment of our global unclassified network was compromised. An opponent was able to gain access to the system. In response to that, I generated an operational requirement not just to push them out of the network, but I wanted to use this opportunity to do a much more foundational review of the entire network, to use this as an opportunity to drive change within my own Service.

Senator INHOFE. What is the administration doing now in response to this attack?

Admiral ROGERS. I'm sorry, I apologize, but I'm not in a position to comment.

Senator INHOFE. In my opening statement I quoted General Fraser. He testified last year that the number of cyber-attacks on TRANSCOM had doubled from 45,000 in 2011 to nearly 100,000 in 2012. Now, that's not very good, is it? Does that concern you, and to what level, General Selva?

General SELVA. Senator, in my current position as Air Mobility Command Commander I'm aware of those statistics. We've taken pretty aggressive action to secure our networks. As I discussed before, the nature of our network that ties us to commercial providers of transportation requires us to have access to the information from their networks as well, and we have been working diligently with those contractors and commercial providers to secure those networks.

The number of attacks doesn't actually equate to the number of actual intrusions and data exfiltrated, but to the number of probes and attempts to get into the network. If confirmed for the position of TRANSCOM Commander, I'll continue to work that issue hard with Admiral Rogers' team at CYBERCOM as well as with our 24th Air Force team, which is the designated unit that essentially provides the external security for our networks.

Senator INHOFE. All right. When we had a hearing on February 27—General Alexander and I have become good friends over the years and we've had a chance to have a lot of conversations, personal conversations—he was asked when a cyber-attack is actually an act of war and to explain what sort of actions an adversary might take in crossing that threshold. He answered that he believes that if an attack destroys military or government networks or impacts our ability to operate, you have crossed that line.

Admiral Rogers, do you agree with his characterization?

Admiral ROGERS. I would agree.

Senator INHOFE. Do you agree that they've crossed that line?

Admiral ROGERS. I'm sorry? The "they"?

Senator INHOFE. They have crossed that line in the actions that they have taken?

Admiral ROGERS. What "they" you're referring to, sir?

Senator INHOFE. I'm talking about, when General Alexander was asked when a cyber-attack does cross that line and become an act of war, and he said that, impacts our ability to operate, you have

crossed that line. Do you agree with that characterization and do you believe that we've crossed that line?

Admiral ROGERS. No, I do not believe we have crossed that line.

Senator INHOFE. Do you agree with the statement that was made by General Selva that the number of attacks, cyber attacks against TRANSCOM, doubling from 45,000 in 2011 to nearly 100,000 in 2012 doesn't properly express our deterrent against these attacks? Does this concern you, that we have doubled in that period of time in the number of cyber-attacks on us?

Admiral ROGERS. I apologize. Is your question to the General or myself, sir?

Senator INHOFE. The question is for you. I'm saying that General Fraser testified that the number of cyber-attacks on TRANSCOM, or let's say cyber-attacks period, has increased from 45,000 to 100,000 in a period of a year. Isn't that concerning? Doesn't that mean that perhaps we're not doing the job we should be doing?

Admiral ROGERS. It is concerning. I think it's reflective of the level of investment that the Department is making in this cyber mission set. Even as we face challenging budget times, cyber remains one of the areas in which the Department remains committed to actual growth in capability.

Senator INHOFE. My only concern here is that, first of all, I believe a lot of the things that I've gotten from the unclassified media and classified media, that Iran is very active in this area. I've been concerned about their capabilities and I've expressed that concern, and it appears to me that a statement such as we have from the administration, "If Iran seizes this opportunity and chooses to join the global community, then we can chip away at the distrust that exists." I just think that we need to be talking about the fact that we have an enemy out there, and he's demonstrated that very clearly.

A few years ago nobody knew what a cyber attack was. But I think we all understand now it can be just as critical, just as damaging to our country, as an attack with weapons on this country. I think you all agree with that, don't you?

Admiral ROGERS. Yes, sir.

Senator INHOFE. Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Inhofe.

Senator Udall.

Senator UDALL. Thank you, Mr. Chairman.

Good morning, gentlemen. Thank you for your distinguished service to our Nation.

Admiral Rogers, I want to turn to you and your written testimony and advance policy responses. In those, I noted that you stated if the Government could continue to access phone records through phone service provider repositories that could serve as a viable alternative to the current bulk phone records collection program. I was glad to read that.

You also wrote that the business records 215 program, "grew out of a desire to address a gap identified after September 11," since one of the hijackers, Khalid Al-Midhar, made a phone call from San Diego to a known al Qaeda safe house in Yemen. You noted that the NSA saw that call, but it could not see the call was coming from an individual already in the United States.

I'm concerned by the implication that somehow the section 215 program could have prevented September 11 and I want to set the record straight from my point of view. As the 9/11 Commission pointed out, the Central Intelligence Agency knew about Al-Midhar, but did not tell the Federal Bureau of Investigation. So the argument that business records data could have been the key to identifying Al-Midhar doesn't stand up in my view.

Also, I don't know why the NSA couldn't have gained the authorization on an individualized basis to determine whether this Yemeni number was in contact with anyone in the United States, and I don't see why a bulk collection authority would have been necessary.

As I'm sure you'll agree, the Constitution is not an impediment to our security; it's the source of our security. We can end bulk collection and focus on terrorists and spies without infringing on the constitutional rights of law-abiding Americans. Last year the President acknowledged what I've been saying: The status quo must change. I look forward to working with you to make those changes.

If I might, in looking ahead I want to turn to the 702 program and ask a policy question about the authorities under section 702. It's written into the Foreign Intelligence Surveillance Act (FISA). The committee asked your understanding of the legal rationale for the NSA to search through data acquired under section 702 using U.S. person identifiers without probable cause. You replied that the NSA court-approved procedures only permit searches of this lawfully acquired data using U.S. person identifiers for valid foreign intelligence purposes and under the oversight of the Justice Department and the Director of National Intelligence.

The statute's written to anticipate the incidental collection of American communications in the course of collecting the communications of foreigners reasonably believed to be located overseas. But the focus of that collection is clearly intended to be foreigners' communications, not Americans'.

But declassified court documents show that in 2011 the NSA sought and obtained the authority to go through communications collected under section 702 and conduct warrantless searches for the communications of specific Americans. My question is simple: Have any of those searches ever been conducted?

Admiral ROGERS. I apologize, sir, that I'm not in a position to be able to answer that as the nominee. But——

Senator UDALL. Yes?

Admiral ROGERS. But if you would like me to come back to you in the future, if confirmed, to be able to specifically address that question, I would be glad to do so, sir.

Senator UDALL. Let me follow up on that. You may recall that Director Clapper was asked this question at a hearing earlier this year. He didn't believe that an open forum was the appropriate setting in which to discuss these issues. The problem that I have, Senator Wyden's had, and others is that we've tried various ways to get an unclassified answer, simple answer, a yes or no to the question. We want to have an answer because it relates, the answer does, to Americans' privacy.

Can you commit to answering the question before the committee votes on your nomination?

Admiral ROGERS. Sir, I believe that one of my challenges as the Director, if confirmed, is how do we engage the American people and by extension their representatives in a dialogue in which they have a level of comfort as to what we are doing and why. It is no insignificant challenge for those of us with an intelligence background, to be honest. But I believe that one of the take-aways from the situation over the last few months has been as an intelligence professional, as a senior intelligence leader, I have to be capable of communicating in a way that highlights what we are doing and why to the greatest extent possible.

Perhaps the compromise is, if it comes to the how we do things and the specifics, those are best addressed perhaps in classified sessions, but that one of my challenges is I have to be able to speak in broad terms in a way that most people can understand. I look forward to that challenge.

Senator UDALL. I'm going to continue asking that question, and I also look forward to working with you to rebuild the confidence, as you pointed out, that the public has in the very vital mission that you have.

If I might, let's turn to cyber for the last half of my time. Before I ask a specific question—and I don't want to steal Senator McCain's thunder, although that's impossible, to steal Senator McCain's thunder. I think he has a very creative idea in setting up a special committee on cyber security, so that we could cut through some of the jurisdictional tensions that exist.

In a more specific context, you noted in your comments that we have to really work to develop and train a significant number of highly capable cyber personnel to meet the Nation's needs. There's no doubt if we're going to achieve dominance that we have to have those personnel. We've done it in the physical world and in the kinetic world, and we can do it in cyber space. Do you believe we're doing enough to cultivate cyber professionals in the early stages of their career?

The Air Force Academy, which is located in my State, has given cadets the opportunity to fly small aircraft in their college years. They enter pilot training then already familiar with the fundamentals and the feel of flying an airplane or a helicopter. I'm afraid we're not giving that same level of attention to cyber training programs. Should we be investing in more hands-on real world training opportunities at our academies for the next generation of cyber warriors?

Admiral ROGERS. Yes, sir. As a naval officer, currently as the Navy component commander, I have worked with our own Naval Academy on doing just that. In fact, right now the requirement at the Naval Academy is there is a baseline cyber course requirement for every midshipman to graduate from the Naval Academy now. That's a new requirement laid down within the last couple of years.

Senator UDALL. I look forward to working with you in that area as well, because we will achieve dominance, but we have to make those investments upfront. I think you and I violently agree.

Admiral ROGERS. Yes, sir.

Senator UDALL. Thank you again, both of you, for your willingness to serve in these important positions.

Thank you.

Chairman LEVIN. Thank you, Senator Udall.

Senator McCain.

Senator MCCAIN. Thank you, Mr. Chairman.

I thank the witnesses for their outstanding service. Just to follow up, Admiral Rogers, General Alexander when I asked, he said because of the overlapping jurisdictions of many committees of Congress that he thought that a select committee to investigate this entire issue, which covers a wide spectrum, would be a good idea. Do you have a view?

Admiral ROGERS. Sir, steps which would try to bring together those focused——

Senator MCCAIN. I would ask if you have a view on whether we should have a select committee or not, Admiral. I'm not used to obfuscation here, okay? Let's not start out that way. Would you or would you not agree that a select committee would be a good idea?

Admiral ROGERS. Yes, sir.

Senator MCCAIN. Thank you.

General, are you on track to remove all the necessary equipment and armaments from Afghanistan by the end of 2014 that you are tasked to do?

General SELVA. Yes, sir.

Senator MCCAIN. You are confident?

General SELVA. Yes, sir.

Senator MCCAIN. You're on track right now?

General SELVA. Yes, sir.

Senator MCCAIN. Thank you.

Admiral, I want to bring up this issue again of the Iranian hack of Navy computers. According to a Wall Street Journal article, the Iranian hack of the Navy's largest unclassified computer network reportedly took more than 4 months to resolve, raising concern among some lawmakers about security gaps exposed by the attack.

The paper reported that the hackers were able to remain in the network until this past November. That contradicts what officials told the Journal when the attack was first publicly reported this past September. At that time, officials told the paper that the intruders had been removed. "'It was a real big deal,' a senior U.S. official told the Journal. 'It was a significant penetration. It showed a weakness in the system.'"

Can you help out the committee on that whole scenario here?

General SELVA. Yes, sir. It was a significant penetration, which is one of the reasons why over the last few months multiple updates to staffers on this committee, because one of the things I wanted to do was, how do we learn from this, how do we work hard to make sure it doesn't happen again. As a result, I directed a rather comprehensive operational response to that. That response was much broader than just be able to come back and say they're not there anymore. I wanted to use this as an opportunity to try to drive change. We put a much more comprehensive, much longer term effort in place than if I had just said, I want to immediately remove them. I wanted to do more than that.

Senator MCCAIN. Was the damage done in your view, significant?

General SELVA. I'm not sure that I would agree with significant, but it is of concern, because in this case they did not opt to engage

in any destructive behavior. My concern from the beginning was, what if they had decided that was their intent?

Senator MCCAIN. I thank you.

Admiral, we have a real problem here, at least from the standpoint of those of us who feel that our ability to monitor the behavior of possible attackers of the United States of America is vital. Mr. Snowden has done some really significant damage. There were polls in the January Quinnipiac Survey, 57 percent of Americans branded Mr. Snowden as a whistleblower, and 34 percent called him a traitor.

A Fox News poll taken the same month found 68 percent of Americans were glad to know about the NSA programs Snowden revealed, while CBS' survey found those disapproving of Snowden's conduct outnumbered those approving 54 to 31. Still, it's a very significant number of Americans that view Mr. Snowden as a whistleblower and a significant portion of Americans as a patriot and approve of his conduct.

What do you think we need to do to counter that impression the American people have, when I'm sure that you and I are in total agreement that this individual violated a solemn oath that he made not to reveal this information and has damaged our ability to defend this Nation?

Admiral ROGERS. Yes, sir, I would agree with your assessment. I think in general there's a couple things here. The first is this idea of transparency, as Senator Udall mentioned, this idea that we have to have a dialogue that talks about what are we doing and the why.

In addition, we have to ensure strict accountability on the part of the NSA. We have to make sure that we do in fact follow those processes appropriately, and when we make a mistake, if we fail to meet those requirements, that we're very upfront about how and the why.

Senator MCCAIN. Do you have any thoughts about the allegations that the FISA courts are just a rubber stamp for the administration?

Admiral ROGERS. I don't believe that to be the case.

Senator MCCAIN. Do you believe that they are exercising sufficient oversight?

Admiral ROGERS. Yes, sir.

Senator MCCAIN. Do you appreciate the fact that we have, at least with a large number of Americans and people around the world, a significant problem with the public relations aspect of the work that you and your organization will be doing?

Admiral ROGERS. Yes, sir, which is why, for example, while my personal opinion is that the FISA structure has worked well, I am open to the idea that, with the view of instilling greater confidence, we should look at a range of potential options to improve that transparency.

Senator MCCAIN. If I had a recommendation for you it would be as much as possible, given the aspects of national security, that you give some speeches in various venues where you could explain better to the American people exactly what you're doing, perhaps not exactly what you're doing, but why you're doing it, and these

threats, including this one that hacked into the Navy on your watch, which I doubt if hardly any Americans are aware of.

I don't think Americans are aware of the extent of the penetration that is not only accomplished, but being attempted, by our adversaries and potential adversaries around the world. Do you agree?

Admiral ROGERS. Yes, sir, I think you're correct.

Senator MCCAIN. Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator McCain.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman.

Thank you both for your service to our Nation in the past and for what you're going to be doing in the future in very demanding and critical jobs. Thank you to your families as well.

Admiral, the White House recently announced the creation of a voluntary framework to establish a cyber-security guide for organizations involved in running the Nation's critical infrastructure. This effort and framework standardizes the cyber security defensive measures to assist in identifying, protecting, detecting, responding to, and recovering from potential intrusions.

How effective do you think that this voluntary framework will be in protecting us from cyber-attack, and what additional measures should the Senate or the NSA take?

Admiral ROGERS. Sir, I think it's a step in the right direction, but I do believe that in the end some form of legislation which addresses both the requirement and need to share information, as well as trying to address the issue of setting standards for critical infrastructure for the Nation, in the long run is probably the right answer. If confirmed, I look forward to working along with a host of other people who would be a party to that.

Senator BLUMENTHAL. I agree with you very, very strongly that legislation will be necessary. There have been efforts to achieve it, bipartisan efforts, I should emphasize, and some of them have been opposed by representatives of the business community on the ground that either there's no need for it, there's no urgency, or other reasons that I think are specious.

I thank you for your offer of cooperation and I look forward to working with you. How urgent do you think it is that we have this kind of legislation?

Admiral ROGERS. The sooner the better. It's only a matter of time, I believe, before we start to see more destructive activity and that perhaps is the greatest concern of all to me.

Senator BLUMENTHAL. Are there areas of our private defense industrial base or even financial, utilities, and so forth that you regard as most vulnerable?

Admiral ROGERS. There's certainly core infrastructure that's critical for us as a Nation. In an unclassified forum I'd be leery of providing specific insights as to where do I think the greatest vulnerability is, but I would be glad to discuss that.

Senator BLUMENTHAL. If the chairman at some point does have a briefing in another setting, a more classified setting, that may be an area that I'd like to explore with you. Thank you.

Let me shift to the role of the National Guard in cyber security. The CYBERCOM Commander, General Alexander, frequently

talked about the critical value of the National Guard as a resource and the role that it could play in expanding our military cyber warfare and defense capabilities. Do you agree with him and how would you define the value that the National Guard can bring to this effort?

Admiral ROGERS. Yes, sir, I do agree. At the present, the Department as a matter of fact is in the process of doing the analysis right now to address that very question. If confirmed, I'll be a part of that process and I intend to dig deeper into it, because one of my take-aways after 30 months right now as the naval commander, if you will, for General Alexander in the cyber mission set is that in the end this is about how do you build an integrated team that harnesses the power and the expertise of every element of that team.

While the U.S. Navy does not have a Guard structure, the Reserve structure we use has been very effective for us. I have worked hard to try to apply it in my current duty.

Senator BLUMENTHAL. Frequently those members of the Naval Reserve or of the Army National Guard or the Air Force National Guard bring capabilities, training, education, skills that are very valuable.

Admiral ROGERS. Oh, yes, sir.

Senator BLUMENTHAL. Turning to another area, if I may, the use of contractors. Following up on the very important questions asked by my colleague Senator McCain, just to state the obvious, here was a contractor who was entrusted with responsibilities that never should have been, and I think many of us are concerned by the scope and scale of the use of private contractors even to screen and evaluate other contractors.

Are you concerned?

Admiral ROGERS. Yes, sir, I share your concern. If confirmed, this is an area that I think I need to ask some hard questions. Why are we where we are today? What led us to this, and are we comfortable with the position we find ourselves in with respect to the role of contractors?

Senator BLUMENTHAL. Are there obvious defects that you can see right away that need to be corrected?

Admiral ROGERS. Nothing comes to mind immediately, although to be honest in my current duties this has not been the same issue on the Navy side that I have seen it on the joint side, as it were.

Senator BLUMENTHAL. Do you think that concern is shared widely in the Intelligence Community?

Admiral ROGERS. I would believe so.

Senator BLUMENTHAL. General Selva, if I can ask you a question, the chairman began by asking some questions about how quickly we need to make determinations about our presence in Afghanistan. What's your assessment now about how flexible we are in determining our timeframe there in drawing down and withdrawing the equipment and personpower that we have?

General SELVA. Senator, today I'd say we have the greatest flexibility that we've had in the past several months. But as each day passes, as you're probably aware, our options decrease. There is a limit to the capacity of the networks to bring that equipment and those personnel out. I will commit to consulting with General Aus-

tin for his assessment and for General Dunford's assessment in ISAF of the specific limits of those networks. In TRANSCOM, our obligation is to make sure that the transportation layer and the distribution layer of those networks is prepared for whatever capacity comes at us.

Senator BLUMENTHAL. Thank you.

My time has expired. I thank you both for your very helpful answers and again for your service. I look forward to working with you.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Blumenthal.

Senator Chambliss.

Senator CHAMBLISS. Thanks, Mr. Chairman.

Gentlemen, to both of you, thank you for your service and your commitment to freedom. We appreciate the great job you do.

I just want to make a comment for the record first, Admiral Rogers, with regard to some comments that Senator Udall made. I don't want to leave a false impression with the American people here that if we had had 702 and 215 in place in 2001 there is a strong probability that we would have been able to determine that a major attack was going to occur, and there's the probability that we would have picked up on conversation between Al-Midhar and those in Yemen with whom he was planning the attack.

Knowing that he was in country versus knowing that he was in communication with terrorists planning an attack are two different things. We didn't have 215, we didn't have 702. We knew that a phone call came to the United States. We did not know it went to San Diego.

It's pretty clear that if we had had more definitive information that we would have gleaned from these programs, that there is strong probability within the Intelligence Community that we might have picked up on that. I won't ask you to make a comment on it, but I want to make sure the record really reflects the actual facts on the ground relative to Al-Midhar.

Now, Admiral Rogers, you and I discussed something that Senator McCain mentioned a little earlier, and that is with respect to trying to communicate these programs to the American people. It's going to be very difficult. He mentioned doing speeches and whatnot. I think you and I agree that that's part of it.

But I'd like for you to elaborate a little bit more on really what you think we can do to show more transparency and to let the American people understand how these programs work.

Admiral ROGERS. As I said, I think we can be a little more communicative with why we're doing this, what led us to these kinds of decisions. I also think it's important that dialogue needs to be much broader than just the Director of the NSA, regardless whoever that individual is. There's a lot more aspects of this discussion than just the intelligence piece.

In the end, this fundamentally boils down to an assessment of risk, both in terms of our security as a Nation as well as our rights as individuals. We value both and we have to come up with a way to enable us to ensure that both sides of that risk coin are addressed. But we should never forget that there's a threat out there that aims to do us harm, that does not have the best interests of

this Nation in mind, and wants to defeat what this Nation represents.

Senator CHAMBLISS. You're exactly right. It's truly unfortunate that General Alexander was put out there on a limb by himself by the administration to seek to explain these programs. While he did a very good job of it, had the President with the bully pulpit been out there with him I think we would have already had a better understanding on the part of the American people of, number one, the misrepresentation of the facts regarding what information is collected on individuals, what's done with that information, and how very difficult it is to be able to access personal information on any single American. It simply is extremely difficult and requires the same process virtually that you would have to go through if you were a U.S. Attorney seeking to get information on an individual American.

The FISA court is not a rubber stamp. All you have to do is look at the makeup of the court, as well as look at the decisions, now which some of them are going to be made public, and I think that's a good idea, as long as we don't reveal sources and methods.

The fact that the administration did not give General Alexander the kind of support they should is really pretty disturbing on my part, and as I mentioned to you yesterday, I have expressed this to the administration. I hope they will give you more support in explaining these programs than they have given to General Alexander, and I have confidence that maybe they will.

Let's talk for a minute about information sharing. We've been working on a cyber bill for years now. We're getting very close to an agreement within the Senate Intelligence Committee between the chairman and myself on a cyber bill that is much needed. One of the key provisions and the last remaining obstacle we have is the immunity provision or the liability protection provision. Would you talk for a minute about your opinion regarding how necessary liability protection is to companies who will share privileged and personal information if we're truly going to have a program that works relative to cyber?

Admiral ROGERS. Yes, sir. I'm not a lawyer, but my sense is it's a critical element in any legislation. I believe to be successful we ultimately have to provide the corporate partners that we would share information with some level of liability protection.

Senator CHAMBLISS. Do you think that firms will participate in the sharing of information if they are not granted pretty much blanket liability protection?

Admiral ROGERS. I would think they'd be much less inclined to do without it.

Senator CHAMBLISS. Thank you very much.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Chambliss.

Senator Donnelly.

Senator DONNELLY. Thank you, Mr. Chairman.

Admiral, thank you. General, thank you, and your families.

The chairman mentioned an article in the New York Times today. I thought one of the interesting quotes was where they said, why would somebody want to be the head of CYBERCOM now? It reminded me very much of the movie Apollo 13 where they said:

This might be one of the worst things that could ever happen to us. They looked and they said: "Well, this could be the best."

This could be the most amazing time, and we have more challenges maybe than ever before. We are giving you the football and expecting big things from both of you on this.

I wanted to ask you, General. In regards to what we have seen in Ukraine and the dealings we've had with Russia before, are you making alternate plans in terms of TRANSCOM as to the work we do with Russia? Are you gaming out worst case scenarios as to how we proceed in the future?

General SELVA. Sir, not yet being in the seat at TRANSCOM, I'd have to say if confirmed that is a priority. I do know as the air component to TRANSCOM and working directly with the TRANSCOM director of operations that we have been building alternative plans. The Northern Distribution Network, part of which flows through Russia, consists of five different options for how we move cargo in and out of Afghanistan. We'll have to look at using other options than the overflight or transit through Russia should the conduct in Ukraine continue.

Senator DONNELLY. I would recommend we get working on that right away, in light of what we have seen going forward these days.

Admiral, when you look at what happened with Mr. Snowden, I know we have done reviews. Have you continued to look and ask what-if about this or about that in regards to where we are now, our operations now, to make sure we are not going to face this again internally?

Admiral ROGERS. As the nominee I haven't done that for CYBERCOM or the NSA, sir.

Senator DONNELLY. Have you thought that through?

Admiral ROGERS. If confirmed, yes, sir, I do believe we need to ask ourselves, so given this compromise, what would be the indicators that would highlight to us, that in fact would point out that now we've been compromised, now we're seeing changes in behavior, and how are we going to have to change that to stay ahead of the threats that face us as a Nation.

Senator DONNELLY. I would suggest that one of the first things you do is sit down and determine where did we go off the highway? How do we fix it? How do we square it away?

One of the areas of interest to me is contractors. You're not in the position yet, but why is it that we have contractors in those positions, as opposed to perhaps military personnel or other Government personnel who are expert in those areas? Is it a lack of individuals who can fill those positions?

Admiral ROGERS. I can't speak to the specifics of Mr. Snowden, the function he was fulfilling, as to why that was chosen to become a contractor vice Government, if you will. But I think it is reflective of a trend over the last decade or so where, as we looked at the size of Government, as we looked at the size of our workforce, some decisions were made that perhaps some of these functions could be executed on a contractor basis vice using permanent Government employees.

I have always believed as a commander that what you should use contractors for are for those functions that are either so specialized that you don't have the capability or skill resident within the Gov-

ernment workforce, whether that be uniformed or civilians, or it is prohibitively expensive to try to achieve that capability, but that what we consider to be core operational functions, those need to be Government.

Senator DONNELLY. In regards to Mr. Snowden's area, will there be a review through all of these contractor areas as to what is core to what we need to do and when we regard and review expense? The next question is what is the expense of what we're dealing with now, with the situations that have been created by Mr. Snowden's conduct?

Admiral ROGERS. I apologize, but I don't know the answer to that.

Senator DONNELLY. No, I understand. I'm just trying to lay out, here are some things as we move forward that we look at.

Mr. Snowden also remarked recently: The U.S. Government has no idea what I have and will not know what I have, and they'll find out as it goes on, in effect, not his exact words. But when we look at Ukraine one of the concerns that has to come up is how much of Mr. Putin's actions were based on knowledge that may have been given to him by Mr. Snowden.

How good a handle do we have at this point on what Mr. Snowden has and what he does not have?

Admiral ROGERS. We have an in-depth analytic effort ongoing within the Department to determine that and ask that question. I haven't been party to that review, although I've seen some of the initial work, which has highlighted where the data he took exactly where it came from. We've tried to identify exactly what the implications are of what he took. That operation is ongoing and will take some period of time to finish.

Senator DONNELLY. In another area, it would be remiss of me not to ask you about supply chain integrity. It's something of concern to me, counterfeit parts, and this would be for both. How are we going to partner with industry? How are we going to work together with our intelligence officials and others to secure the integrity of the supply chain of what we have? We see counterfeit parts in missiles, in planes. It is an extraordinarily dangerous situation, and I was wondering what your plans are as we move forward to try to get this squared away.

General SELVA. Senator, our obligation in TRANSCOM is to work as the distribution process owner under the unified command plan. Part of that obligation is to work directly with the Defense Logistics Agency (DLA) on the issue of supply chain management and integrity of the supply chain. It's out of the lane that I've been in for the last year and a half as the commander of Air Mobility Command. It is one of the areas that I have committed to spend time with with Admiral Hernitchek, to get at the details of the supply chain integrity process.

It's more than just the data. It is in fact the ability of counterfeiters to bring to that market parts that appear to be genuine, but in fact aren't. It's a physical issue as well as a data security issue. It goes right to the heart of our industrial capacity and the ownership of the intellectual rights and being able to produce the products that our soldiers, sailors, airmen, and marines use in battle.

Senator DONNELLY. I would ask you to make that a priority, because we are one counterfeit part away from disaster on a constant basis.

General SELVA. Yes, sir.

Senator DONNELLY. Thank you very much. Thank you both for your service and to your families.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Donnelly.

Senator Ayotte.

Senator AYOTTE. Thank you, Mr. Chairman.

I want to thank both of you for your service to our country, and to your families as well for their support and sacrifices.

General Selva, with regard to DOD's air refueling capability, how important is it to our military capabilities and our national security?

General SELVA. Senator, the capacity of Air Mobility Command to operate at TRANSCOM's behest and provide refueling around the world is critical to being able to move our forces to the places they need to be when they need to be there. The Air Force, as you've probably heard over months and years, talks about global vigilance, global reach, and global power. Tankers are what make us global.

Senator AYOTTE. I'm really pleased the 157th Air Refueling Wing at Pease, the New Hampshire Air National Guard Base, has been chosen as the top Air National Guard unit to receive the new tankers, the KC–46A. I want you to know we had a very positive public hearing for the basing of the KC–46A last week in New Hampshire.

I wanted to ask you, in your role as Commander, Air Mobility Command, what's your assessment of the 157th Air Refueling Wing at Pease? How have they performed and how important is the Guard in all of its capabilities as we go forward?

General SELVA. Senator, the 157th has a pretty storied heritage in the tanker world, and they're a high performing organization. They're one of the units to which we've appended an Active Duty associate unit and the unit is performing quite well. The base and the unit exist in an area of fairly high demand for tanker services and as a result their performance speaks for itself. They're a great unit and we look forward to being able to base the KC–46A Pegasus at Pease, subject to the outcome of the environmental impact statement.

Senator AYOTTE. Fantastic. I think you're going to get a very positive outcome. The whole community is really excited and very supportive of having the new tanker there, and I look forward to working with you on that. It's incredibly important to our national security.

I noted Senator Donnelly asked you about the issue of the Northern Distribution Network with regard to our retrograde from Afghanistan. In light of what's happening in the Ukraine, the President, many of us, are pushing for further economic sanctions, other types of sanctions against Russia for their invasion of Crimea.

If the Russians were to take retaliatory action as a result of that to shut down the Northern Distribution Network with regard to the transit operations on those roads, what impact would that have to

us and how would we address it? Because I think it's something we have to understand and be prepared to address.

General SELVA. Yes, ma'am. If the Russians were to take action to constrain our access to the Russian segments of the Northern Distribution Network, we have other options to move that cargo in and out of Afghanistan. The singular item that moves across that network that would concern me at this point is the subsistence cargoes in the form of food and non-combat articles. I'm told about 20 percent of the subsistence cargoes move through that network. We'd have to use another option to get it in. We do have several options in the Northern Distribution Network that do not include transitting Russia.

Senator AYOTTE. If for some reason, which obviously I would hope that they wouldn't take that type of action, but we'd be prepared to use other options if we had to and could do so?

General SELVA. Yes, Senator, we would.

Senator AYOTTE. Thank you. I appreciate it.

Admiral Rogers, thank you for taking on at a very challenging time this important position. Last week it was reported in the press that Russia is using cyber-attacks against the Ukrainian telecommunications system to block the Ukrainian leadership from accessing the country's phone network. To what extent do you believe Russia is conducting cyber-attacks against the Ukraine, and what could the United States do to help the Ukraine better defend itself against attacks from Russia?

Admiral ROGERS. Ma'am, in an open, unclassified forum, I'm not prepared to comment on the specifics of nation state behavior. Clearly, cyber will be an element of almost any crisis we're going to see in the future. It has been in the past. I believe we see it today in the Ukraine. We've seen it in Syria, Georgia. It increasingly is becoming a norm.

As we work to partner with others to develop norms of behavior and expectations for what is acceptable and what is not acceptable, examples like this highlight to us I think what is not acceptable. As we work with the Ukrainians and other nations to attempt to figure out what's the best way to address them, whether the Ukrainians ask for specific technical assistance, I think we'd have to work through everything on a case by case basis.

Senator AYOTTE. Do you believe we should help our allies in situations like this if they are receiving cyber-attacks, and working with them to combat these attacks?

Admiral ROGERS. Yes, ma'am.

Senator AYOTTE. I think that's very important, particularly with what's happening in the Ukraine right now, that we are active in this area in countering any type of actions by the Russians, cyber-attacks or otherwise.

I wanted to ask you about DOD's vulnerability overall to a cyber-attack. In January 2013, the Defense Science Board issued a task force report titled "Resilient Military Systems and the Advanced Cyber Threat". The report concluded that, "The United States cannot be confident that our critical information technology systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities."

In other words, we're not confident that many of our military systems would work if we were attacked by a high-end peer-to-peer adversary.

Do you share that assessment and how can we make sure that DOD is more resilient to cyber-attacks?

Admiral ROGERS. I certainly share that concern, which is one reason why I believe creating a defensible architecture has to be one of the most important things we do. The reality is the network structure of today reflects a different time and a different place. I have experienced that firsthand in my current duties in the Navy as the operational commander for the Navy's networks. I have watched that challenge across the entire Department.

That's why the Joint Information Environment (JIE) I think is so critical to the future for us. We have to get to a defensible architecture.

Senator AYOTTE. We have to work with you on that.

Finally, there's been a lot of discussion about Edward Snowden here today. Do you believe that the disclosures that he made have potentially put at risk the lives of Americans and our allies, or at greater risk, because he has released this type of classified information?

Admiral ROGERS. Yes, ma'am.

Senator AYOTTE. Yes is the answer to that?

Admiral ROGERS. Yes.

Senator AYOTTE. I think that people need to understand that, that he has put potentially at risk American lives and the lives of our allies. That is very, very important for people to understand in terms of what we are addressing and what we're dealing with and how we characterize his behavior.

Thank you both.

Chairman LEVIN. Thank you, Senator Ayotte.

Senator King.

Senator KING. Thank you, Senator.

General Selva, it's good to see you again. If I was in an airplane out of gas over the North Atlantic, I'd call the guys from Bangor. Forget about those guys from Pease. [Laughter.]

Senator AYOTTE. I don't think so. [Laughter.]

Senator KING. The 101st could take care of you quite adequately.

As you look across the broad range of commercial assets, military assets, that TRANSCOM employs across the globe, what do you feel are the greatest risks and vulnerabilities to TRANSCOM today to execute its responsibilities? How about the vulnerability of commercial carriers to events like cyber intrusions? Going into this new job, what's going to keep you awake at night?

General SELVA. Senator, I think there's probably two things that worry me the most over the coming couple of years. The first is once we have completed whatever retrograde operation happens in Afghanistan, whether we have a residual force or no force remaining behind, the demand signal for lift, surface and air, will diminish significantly. We've already seen in the last year nearly a 50 percent reduction in the requirement for sustainment cargoes into and out of Afghanistan, combat articles as well as just regular sustainment.

That has an implication for our organic fleets, sealift, airlift, as well as surface, and for our commercial partners whose networks we access to make that entire distribution network work. That decline in requirements, a return to a more stable environment, if you will, actually has some negative readiness implications across the enterprise. We're studying those in all of the organic and commercial sectors of the market to try and understand those implications. They have significant impacts on the commercial cargo carriers, both sealift and airlift, who have been such an integral part of that network into and out of Afghanistan.

Senator KING. What percentage of TRANSCOM's assets are organic versus commercial at this moment?

General SELVA. That's a difficult number to quantify, but I'll take a stab at it. Roughly 40 percent of our capacity is organic in the air environment and about 50 percent, if we access all of the available assets through the Civil Reserve Air Fleet (CRAF), would be brought to us by our commercial partners. I don't have the specific statistics.

Senator KING. As the demands of Afghanistan diminish, is there an industrial base issue here in terms of the commercial carriers? Are they going to go away? Are they going to be able to find other business? Is there a risk of not having the capacity when we need it?

General SELVA. There are two dynamics at play, Senator, in that environment. One is the health of the airline industry as a whole, both commercial cargo carriers and commercial passenger carriers, and two segments within that, that industry, the charter carriers and the scheduled carriers.

The decline in the demand signal on those commercial carriers will change the economics of that industrial segment. The second thing that's changing is the very nature of commercial charter cargo across all of the global economy. With the introduction of large aircraft with large cargo bays below the passenger decks, we now see commercial passenger carriers reentering the charter cargo market. That has changed the dynamic of our CRAF partners and we have to understand the impacts of that change in the economy on their capacity to be with us in crisis.

Senator KING. That's an issue that we're just going to have to watch as it evolves?

General SELVA. Yes, sir. To be fair, right now we have an ongoing study. We're about a year into working with our commercial partners to understand the economic dynamics of what's changing in the cargo and passenger markets. We are right now in about a 3-month period of receiving their comments on the work we've done. We owe this committee a report in mid-June, if I understand correctly, on the outcome of that discussion.

Senator KING. Thank you.

Admiral Rogers, I'm going to ask a question that I don't think you're prepared to answer, but I may ask it again in a year. I've been in a number of hearings both in the Intelligence Committee and in this committee on cyber issues, CYBERCOM and the NSA. How can you possibly do both of these jobs?

Admiral ROGERS. There is no doubt it's a challenge, and I'll be in a much better position, as you indicate, if confirmed, to look

back and say how hard has it been and what have been the challenges. But I just believe that where we are right now, many of the missions and functions are so intertwined and related that to not do it this way would create real concern. Right now, in my current duties in the Navy I work for General Alexander both as CYBERCOM and as NSA leader, and so I have experienced these same challenges firsthand within my own service.

Senator KING. But you understand how over the past year both jobs have grown in responsibility. You have to be a spokesman, you have to manage. I just think it's something that we're going to really have to think about along with the administration going forward. I understand the desire to have it in one person, but, boy, I would think running the NSA itself is more than a full-time job.

Admiral ROGERS. We'll be busy, sir.

Senator KING. One of the major issues that we've been discussing again for the past year and a half, actually for the past, I don't know, years before I was here, is the necessity of some kind of cyber legislation that allows better coordination between the private sector and the Government. How do you assess the importance of that kind of legislation coming out of this Congress?

Admiral ROGERS. Sir, I believe that legislation is a key for our future. We have to change the current dynamic.

Senator KING. I certainly hope people are listening around here, because ever since I've been here everybody's been saying that, but it doesn't seem to change. My father used to say if you drove straight at the Pentagon it kept getting further and further away. I feel like that's where we are with this legislation. Everybody's talking about it. I certainly hope you'll work with us to try to develop that legislation in the multiple committees that have jurisdiction.

I believe one of our greatest vulnerabilities is to cyber-attack. I think the next Pearl Harbor is going to be cyber. The problem is we're more vulnerable than many other places. It's an asymmetrical disadvantage because we're so advanced in terms of our linked-up, networked society. How do we prevent that or what are the tools and are we where we should be? I certainly don't want to have a hearing or a set of hearings here about why we were asleep at the switch.

Admiral ROGERS. I think clearly we're not where we want to be. We're generating capability, we're generating capacity, and those are all positive steps in the right direction. But in the end I believe we have to get to some idea of deterrence within the cyber arena.

Senator KING. I think you're absolutely right about that, and we have the whole strategy of deterrence on the nuclear side and I think we have to develop a strategy of deterrence on the cyber side, that if somebody comes into our networks they're going to have some serious problems with their networks.

Thank you, Admiral.

Chairman LEVIN. Thank you, Senator King.

Senator Lee.

Senator LEE. Thank you, Mr. Chairman.

Thanks to both of you for joining us today and for your service to our country. Admiral Rogers, I thank you in particular for vis-

iting with me in my office. I appreciated the opportunity to discuss those important issues.

There does have to be a balance struck between achieving our national security goals and protecting the constitutionally guaranteed rights of American citizens. Ultimately, I agree with my friend Senator Udall that, properly understood, these two things are the same thing. Our security lies in our constitutional protections and so we can't overlook constitutional protections in the interest of national security without compromising a good deal of what is embodied in our national security interests.

In our well-intended efforts to recover and move forward past September 11, 2001, we have at times tried to strike a balance in a way that I find troubling. As I've stated before, I have some pretty deep-seated concerns with some of the things that have been revealed in recent months to the public, things that previously were known only to Members of Congress and to other people with the right security clearance within the Government.

I worry about the NSA's surveillance and metadata collection programs and the risks that such programs could pose to the constitutionally protected rights of American citizens. The Fourth Amendment stands to safeguard those rights, and even if one assumes for purposes of this discussion that currently the only people employed at the NSA are people with only our best interests at heart, we still run a risk, even if that assumption is made, that at some point in the future, whether it's a week from now, a month from now, a year from now, 10 or 20 years from now, unless we have the right safeguards in place those powers will be abused. They will be abused with respect to American citizens.

Particularly given the fact that the NSA's mission is related to foreign intelligence-gathering, we need to make sure that we protect American citizens in their constitutionally protected rights.

Admiral Rogers, if confirmed to this position how would you work to protect the constitutionally protected rights of American citizens while doing your job?

Admiral ROGERS. Yes, sir. I would attempt to be as transparent as possible with the broader Nation about what we're doing and why. I would try to ensure a sense of accountability in what the NSA does. The Nation places a great deal of trust in this organization. It has an incredibly important mission. It's a mission that involves a tension in our society, given the fact that the fundamental rights of the individual are so foundational to our very concept of the Nation.

I welcome a dialogue on this topic. I think it's important for us as a Nation. I look forward to being part of that dialogue. As you and I have previously discussed, I am committed to trying to be a good partner in that effort.

Senator LEE. I understand that a certain level of confidentiality must almost unavoidably surround many of the NSA programs that might be of concern to the American people, to ensure the effectiveness and to keep our enemy actors from working around our systems. But the public has developed a certain distrust of many of those programs.

In discussing this concept with Senator McCain a few minutes ago, you mentioned that there might be a range of options avail-

able to us. Can you describe what some of those options might look like in balancing the need for confidentiality on the one hand, in order to protect our programs, and the need for transparency on the other?

Admiral ROGERS. I'd be looking at what are the mechanisms we use to assess the value portion of this and how can we do this potentially in a more public way. I haven't fully formed my own thoughts in this regard, but I think it's something that's incredibly important and I think is very specific to the duties as the Director of the NSA, if confirmed, the ability to be able to lead an honest and open dialogue about just what is the value of these efforts as we try to move forward.

As I said, I'm not on the job yet. I need to get much smarter, but I'm committed to doing so.

Senator LEE. The President's directed that the Government start to transition out of having the Government itself hold onto the bulk metadata collected pursuant to section 215 of the Patriot Act. Can you give me an update on how that process is going and how it might unfold?

Admiral ROGERS. Sir, as the nominee I haven't been part of that process, so I'm not in a position to give you a sense for how it's unfolding. I know it is ongoing. The President set a deadline of the 28th of March, indicating he wanted feedback on how the best way to move forward was. The issue that's among the many that's important to me as we move forward is this, and we try to figure out the best way, is how do we address the idea of speed, the ability to query the data in a way that both protects the rights of the individual, but also enables us to get answers in a quick, reasonable time period.

Senator LEE. Thank you.

President Obama stated in a speech in January the following. He said: "I've directed the Attorney General to work with the Foreign Intelligence Surveillance Court so that during this transition period the database can be queried only after a judicial finding or in case of a true emergency."

What do you think might constitute a "true emergency" in this context?

Admiral ROGERS. Potential loss of life, hostage, criminal kind of scenarios.

Senator LEE. I assume that in those scenarios there would have to be a time component, an urgency component for that to qualify.

Admiral ROGERS. Yes, sir, I would think so.

Senator LEE. Not a mere inconvenience to the Government personnel involved, but some practical reason that would make it impossible, rather than just inconvenient, to go to the FISA court. Is that your understanding?

Admiral ROGERS. Inconvenience is clearly not the standard that's intended.

Senator LEE. I see my time has expired. Thank you very much, Admiral.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Lee.

Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman.

I want to thank both of you and congratulate you on your nominations. I've read your resumes, quite impressive. Thank you for the service to our great country.

I also want to acknowledge the passing on Sunday, March 9, 2014, of one of your fellow Air Force officers, one of your fellow comrades, if you will, at the Air Force Academy, in the passing of Major General Stewart. We're very sorry for that, and a loss for all of us.

If I can, General Selva, to start with, the equipment in Iraq, where did it go, the equipment that we should have taken out? How much did we leave behind? Where did it go? What have we done with it?

That leads right into what we're going to do in Afghanistan. I'm hearing that we're going to leave so much stuff behind. The State of West Virginia is kind of watching its p's and q's and its pennies, nickels, and dimes. How does that fare?

General SELVA. Sir, I'm not in a position to comment on what we left behind in Iraq.

Senator MANCHIN. Is that because of security?

General SELVA. No, sir. I wasn't party to those decisions.

Senator MANCHIN. Could you get some information on that?

General SELVA. I could try to find out for you.

[The information referred to follows:]

The majority of equipment in Iraq was transported back to the United States or to Afghanistan based on military operational and training requirements. The Department of Defense (DOD) transferred equipment and property to the Government of Iraq (GoI) under a number of authorities to build up the security forces of Iraq. Specifically, DOD transferred $319.7 million (fair market value) worth of foreign excess personal property (FEPP) to the GoI under the authority of title 40 U.S.C. § 704. Examples of these items are installation and base life support equipment (e.g., commercial vehicles, power generators, living containers, security barriers, and air conditioners). DOD achieved an estimated cost avoidance in excess of $605 million by not transporting these items back to the U.S. Additionally, DOD transferred over 24,000 pieces of "excess" equipment under the authority of title 22 U.S.C. § 2321j (grant transfers of Excess Defense Articles) to the GoI. Examples of this equipment are helmets, older version weapons (M16), body armor, tools, and commercial vehicles. DOD also transferred 1,305 pieces of "non-excess" equipment to the GoI under the authority of § 1234 of Public Law 111–84. Examples of this equipment are High Mobility Multipurpose Wheeled Vehicles, 40 ton trailers, maintenance trucks, and airfield support equipment.

Finally, DOD transferred 759 items valued at approximately $10.8 million to 20 different U.S. State and Local organizations through the National Association of State Agencies for Surplus Property. Examples of this equipment are: non-tactical vehicles, light sets, generators, dozers, bobcats, and forklifts. The equipment is provided on an "as-is, where-is" basis to the States, with the States funding all packaging and transportation costs. Items not claimed by any organization were disposed of in Iraq.

Senator MANCHIN. Thank you, sir.

General SELVA. I will let you know that in the current discussions we're having with ISAF on what we might leave behind in Afghanistan, one of the key issues that we have to address is the residual value of the equipment and whether or not the cost of lifting it out of Afghanistan is worth that investment. We have to do that, essentially a business case.

Senator MANCHIN. Do we have any buyers in that part of the world for it or are we just going to give it away?

General SELVA. Sir, in some cases the equipment will be disposed of through foreign military sales. In others it will be through grants. But I don't have the specifics.

Senator MANCHIN. If you could do that, I'd appreciate it.

General SELVA. If confirmed, I will get with the DLA team and get you that information.

[The information referred to follows:]

Equipment that is required to meet future military operational and training requirements is being transported back to the United States. Equipment that is excess to the Department of Defense (DOD) requirements is offered to the Government of the Islamic Republic of Afghanistan (GIRoA) and other eligible countries under various authorities. As of March 30, 2014, DOD has transferred $91 million (fair market value) worth of foreign excess personal property to the GIRoA under the authority of title 40 U.S.C. § 704. Examples of these items are installation and base life support equipment (e.g., commercial vehicles, power generators, living containers, security barriers, and air conditioners). DOD achieved an estimated cost avoidance in excess of $1.1 billion by not transporting these items back to the United States. As with the equipment in Iraq, excess military equipment is made available to GIRoA and other eligible countries on an "as-is, where-is" basis under the authority of title 22 U.S.C. § 2321j (grant transfers of Excess Defense Articles) or title 22 U.S.C. § 2751 (Foreign Military Sales). Non-excess military equipment may be transferred to GIRoA under the authority of § 1222 of Public Law 112–239. DOD is providing lists of excess equipment to the National Association of State Agencies for Surplus Property (NASASP) for potential transfer to U.S. State and local organizations on an "as-is, where-is" basis. To date, no equipment has been requested by NASASP due to the high transportation costs.

Commercial equipment that has no trade security controls may be sold to local Afghan vendors beginning in April 2014. Finally, equipment with trade security controls that is not disposed of in any of the methods above will be demilitarized and disposed of in Afghanistan.

Senator MANCHIN. Admiral Rogers, if you can, give me an overview of the cyber-attacks from Russia, and especially with the Ukraine situation we have right now that we're dealing with, and how that escalates to concerns and maybe more activity into the former Soviet Union countries, such as Kazakhstan and some of the others that are very much concerned, and even Poland, at what's going on. Are you seeing an uptick in those type of cyber-attacks there?

Admiral ROGERS. We clearly see that there's an ongoing cyber element to the challenges in the Ukraine at the moment. In terms of specifics, I would respectfully ask that this is something that would perhaps be best shared in a classified setting.

Senator MANCHIN. Okay. I was just wanting to see, I would assume there has been. If you can do that, I'd appreciate it, sir.

Also, my State of West Virginia has gone through a water crisis, if you will, because of a spill. I've said this before. If anyone wanted to know the effects it has on the population and the concerns and the hysteria—and we had no loss of life, no one seriously ill—what a cyber-attack would do to the confidence of the people, we're a perfect example, if you would come down and work with us and help us on that.

But with that being said, our most vulnerability I see is in our water, our food, and our grid system. Since a lot of this is privately owned or corporately owned, are you interacting and how much are you interacting with those concerned to beef up the security?

Admiral ROGERS. Sir, it's clearly not in my current duties, but if confirmed that would be an aspect of the mission. Absent legislation, we're attempting to do that on a voluntarily-in partnership

basis. Those partnerships in some areas are working very well, in others clearly not as mature as we would like.

Senator MANCHIN. Maybe you can even elaborate more. I know that Senator King had mentioned you probably wouldn't be able to answer it today, you could a year from now. Tell us what all has been thrown into the mix, if you will, of what you're expected and how you can bring everything together with the demands and the growth, I think is what we're concerned about, and if we should still stay under one umbrella? I think right now we're going down that direction. But how much more has been thrown at you?

Admiral ROGERS. Clearly, it's a demanding set of duties. I'd also highlight the Director of NSA and the Commander of CYBERCOM does not operate alone by themselves. There's a strong team in place. I've had the honor of working with that team on both the CYBERCOM side and the NSA side for the last 2½ years in my current duties. They're a real strength for the team.

Senator MANCHIN. It's amazing to me—and I don't see this in West Virginia at all—they're trying to lift Snowden up to any type of hero. He is basically a traitor in our eyes and what he's done to our country.

But with that being said, there had to be a frustration level to where he felt, he felt that that was the direction for him to go, because there was no outlet. Are you able to in your new position looking at how you can work, because you're going to have contractors involved and it looks like you're going to have more contractors—are they able to come and have their concerns and do you have any type of an outlet there that would work with them, so that we don't continue to go down this road?

Admiral ROGERS. Yes, sir, there are avenues both within the NSA chain of command, there are avenues both with an inspector general structure, both within NSA and CYBERCOM as agencies.

Senator MANCHIN. Did Snowden ever take those avenues and try to air his concerns?

Admiral ROGERS. I don't know, but I'm sure in the ongoing investigation as we review the particulars of the Snowden case that'll be one of the questions of high interest.

Senator MANCHIN. Yes, because basically he just went down the sabotage route. You've said before some of the things he's done and has continued to do is irreparable.

Admiral ROGERS. I'm not sure I said irreparable, but I believe it has significant risk, damage, and consequences for us.

Senator MANCHIN. Would you look at him as a traitor?

Admiral ROGERS. I don't know that I would use the word traitor, but I certainly do not consider him to be a hero.

Senator MANCHIN. Thank you.

Chairman LEVIN. Thank you, Senator Manchin.

Senator Graham.

Senator GRAHAM. Thank you both for your service and I look forward to working with you in the future. I have every confidence that you'll be confirmed, and these will be difficult, but I think very rewarding, jobs.

General, on the transportation side, what effect will sequestration have on the ability of Air Transportation Command to meet our defense needs over the next 8 years?

General SELVA. Senator, I think there's two significant impacts sequestration will have. The first will be as an industrially funded organization, where our users that use transportation services pay out of their operation and maintenance (O&M) accounts for those services, the decrease in the availability of those funds is likely to cause a decrease in that demand signal. The corollary to that is that will force then our organic capacity, the training and seasoning of the people that do that work, whether it's Military Sealift Command or Air Mobility Command, to spend more of their O&M dollars to achieve that training they could as a byproduct of moving transportation requirements around the world. There is a bit of a two-sided coin there on the impact of sequestration on the readiness of those fleets.

Senator GRAHAM. In simpler terms, would it be really damaging?

General SELVA. Yes, sir.

Senator GRAHAM. From an Air Mobility Command point of view, which you are very familiar with, how has our air fleet been affected by the operational tempo (OPTEMPO) over the last 10 years?

General SELVA. Senator, we've had a fairly high OPTEMPO, particularly in our airlift and air refueling fleets. The fleets are holding up pretty well. We do a continuous assessment of the structures in our large airlift aircraft. But the OPTEMPO is showing its——

Senator GRAHAM. Is it fair to say that when we accepted each plane into the fleet—the operational tempo has been really unprecedented since World War II probably, and that when it comes time to evaluate our future needs, we're flying the wings off of these planes basically? I know they're structurally sound, but I want the committee to understand that no one envisioned this level of operational tempo before September 11, and we're going to have to make accommodations for it.

Admiral, are we at war?

Admiral ROGERS. I wouldn't use the word war, but there is no doubt we are in a conflict.

Senator GRAHAM. If it's not a war what is it?

Admiral ROGERS. War has a very——

Senator GRAHAM. Is it a disagreement?

Admiral ROGERS. I apologize, Senator. I didn't understand the question.

Senator GRAHAM. I said, are we at war? You said, no, I think it's something else, conflict. How could you say we're not at war?

Admiral ROGERS. War has a very specific legal definition and I don't believe we've met that.

Senator GRAHAM. Do you believe that we're at war with al Qaeda and their affiliates?

Admiral ROGERS. Yes, sir. Senator, if I could, I apologize. I assumed you were talking in the cyber arena. Please accept my apologies.

Senator GRAHAM. Absolutely. My bad, my bad.

Admiral ROGERS. Yes, sir, there is no doubt——

Senator GRAHAM. No, I got you. You don't want to go down the road. I got you, no.

But we are at war in terms of radical Islam being the enemy of the Nation?

Admiral ROGERS. Yes, sir.

Senator GRAHAM. The NSA program is designed to protect us against an enemy who is hell-bent on attacking our Nation at home and throughout the world, do you agree with that?

Admiral ROGERS. Yes, sir.

Senator GRAHAM. Is it likely that there are fifth column movements already in the United States, embedded in our country, sympathetic to the enemy?

Admiral ROGERS. We've seen those kinds of actions by people in the United States sympathetic to that previously.

Senator GRAHAM. Do you believe if we had had the NSA capabilities in effect in September 2001 that we have today there's a high likelihood that we would have intercepted the attack on September 11?

Admiral ROGERS. The potential certainly would have been much greater.

Senator GRAHAM. As we reform the program, will you keep in the forefront of your thinking not to take us back to pre-September 11 capabilities?

Admiral ROGERS. Yes, sir.

Senator GRAHAM. When it comes to monitoring content of an American citizen on a phone, the NSA program is very restrictive in that regard; is that a true statement?

Admiral ROGERS. Very restrictive, sir.

Senator GRAHAM. The threat we face is very real. Major Hassan, are you familiar with that gentleman?

Admiral ROGERS. At Fort Hood, I believe, yes, sir.

Senator GRAHAM. How could he, a major in the U.S. Army, communicate on the Internet with Anwar Awlaki, a leader of al Qaeda in Yemen, an American citizen, and we not understand that or not find out about, detect that? Do you know?

Admiral ROGERS. No, sir, other than to say in general I believe he took advantage of the protections afforded to our citizens.

Senator GRAHAM. Could you do me a favor and evaluate how we missed Major Hassan? Because I believe in privacy and transparency, but I believe that any system that's going to protect America from an attack has to be able to pick up a communication from a major in the U.S. Army with one of the leading terrorists in the world. If we can't do that, something's wrong. Would you please go back, evaluate how we missed Major Hassan? If we need to change the law to catch future Major Hassans, I would like to help you in that endeavor.

[The information referred to follows:]

Many factors contributed to the outcome of the 2009 Fort Hood incident and I'm not in a position to identify the specific or primary ones. This has been the subject of extensive study by the Department of Defense Independent Review Panel and by the Senate Homeland Security and Government Affairs Committee and I refer you to the reports that detail their respective investigations into the Fort Hood shooting and recommendations to prevent future incidents. Both reports are authoritative and comprehensive.

Senator GRAHAM. The Boston attack. Is it fair to say that our ability to pick, intercept communications, identify the perpetrators

fairly quickly, gave us some lead time about anything they may have been planning in New York?

Admiral ROGERS. Yes, sir.

Senator GRAHAM. When it comes to being at war with radical Islam, do you consider the Homeland one of their chief targets?

Admiral ROGERS. Yes, sir.

Senator GRAHAM. If they could attack any place in the world, the top priority would probably be here at home?

Admiral ROGERS. Yes, sir.

Senator GRAHAM. Now, when it comes to reforming this program, how much can we talk about how the program works before we destroy its ability to protect us?

Admiral ROGERS. There's clearly always an element there that we don't want to divulge sources and methods.

Senator GRAHAM. Would you say that the discussions about how this program works and the details probably have already helped the enemy in terms of being able to adapt?

Admiral ROGERS. It's given them greater insights into what we do and how we do it.

Senator GRAHAM. Is it fair to say that the enemy, when they communicate, uses commercial networks like the rest of us?

Admiral ROGERS. Yes, sir.

Senator GRAHAM. The only way we'll be able to detect what they're up to is to be able to access these commercial networks in a reasonable fashion?

Admiral ROGERS. Yes, sir.

Senator GRAHAM. Do you agree with me that the only way to deter them is to prevent them from attacking us, because killing them is not a deterrent? They welcome death. The best way to protect us against radical Islam is to find out what they're up to and hit them or stop them before they hit us? Is that the world in which we live in?

Admiral ROGERS. Yes, sir.

Senator GRAHAM. Thank you.

Chairman LEVIN. Thank you, Senator Graham.

Senator Reed.

Senator REED. Thank you very much, Mr. Chairman. Thank you, gentlemen and your families, for your devoted service to the Nation.

Let me begin with General Selva. General, one of the important components to TRANSCOM is the CRAF. Your agency is studying the relationships and what we do now, as we reset after significant extensions in Afghanistan and Iraq and around the globe. Can you give us an idea, a preliminary idea at least, of what we have to do to ensure the CRAF program continues to support our wartime needs, and any highlights of the study that are ready for prime time?

General SELVA. Senator, inside the relationship with the CRAF we have 28 separate carriers that provide cargo and passenger services, each with their own business plan, each with their own motivation for how they run their businesses. Part of the study was to get at the eachs of how the industry runs and get at the broad macroeconomics of how the industry is going to evolve over time.

We've put those two big pieces together. We're now working with the senior executives in those individual carriers to come to some agreement on what a contract mechanism might look like to incentivize their volunteer service in the CRAF. As you may be aware, the policy that governs how we manage, National Airlift Policy, was last updated in 1987. This study is the first major effort post-Desert Storm to get at what the economics of the industry look like and how they affect our relationship with the CRAF.

I fully expect, based on my interaction with senior executives from many of the airlines, that their volunteerism will continue. The question is how do we make it a meaningful business incentive for them to do that.

Senator REED. Do you anticipate any legislative requirements that you would have that would help you achieve a more efficient outcome for the Government?

General SELVA. Senator, based on the preliminary work we've done in the study and our interaction with the carriers, I don't believe any legislative changes are required to the National Airlift Policy to make us successful.

Senator REED. But if they do, you will inform us?

General SELVA. Yes, sir, absolutely.

Senator REED. Thank you.

Admiral Rogers, congratulations. I don't know if that's in order or not, but congratulations.

Admiral ROGERS. Thank you.

Senator REED. You have two huge responsibilities, CYBERCOM, which is a DOD function, and the NSA. In your organization are you going to have, or are you contemplating having, principal deputies that would essentially focus exclusively on one or the other?

Admiral ROGERS. Yes, sir. Each organization has its own deputy and a complete operational organization.

Senator REED. There are no changes at this time in those deputies?

Admiral ROGERS. I believe you may see the CYBERCOM deputy changing in the course of the next few months. But that's again part of the normal rotation.

Senator REED. Part of the anticipated rotation, et cetera. There'll be the overlap, et cetera.

Let me change gears slightly. We've all recognized the growing importance of cyber in every capacity, and I think the lessons of history suggest that the more we practice the better we are when the game starts. To my mind, I don't think we've had the kind of coordinated exercises between CYBERCOM, the NSA, the Department of Homeland Security, every other agency, which basically would confirm what we believe and maybe give us some surprises about what we don't know. Is that your impression, too?

Admiral ROGERS. I think we've done a good job of exercising within the Department. As we bring more capability, more capacity, on line, I think the next major evolution for us is how do we exercise more broadly across the U.S. Government in applying those capabilities.

Senator REED. Then also there's the issue of not only across the U.S. Government, but also reaching out to utilities, both financial utilities and public utilities. Is that something where again you

would need either funding or authorization or encouragement from Congress?

Admiral ROGERS. At this stage of the game, I don't know. But I do make the commitment that if I am confirmed I will assess that, and if I believe that money or authorities or support from the legislative side is required I will approach you.

Senator REED. I would encourage you to do that, because again I think there are so many different moving parts in these issues that you're addressing, not just in terms of operational, but privacy, constitutional, policy, commercial enterprises versus Government enterprises, not-for-profits, that I think this exercise would be hugely important. This is probably not the most precise analogy, but when we saw war beginning in 1939 and 1940 we learned a lot in the Louisiana maneuvers. In fact, we discovered some very capable leadership down there that was in the junior ranks and vaulted over some others very quickly when the war started.

I don't sense we've actually done that in the scale that we talked about. I would urge you to look very quickly and get back to us very quickly in terms of what we have to do to assist you.

Again, I think both of you gentlemen bring extraordinary dedication and service, and not just yourselves personally but your families. Also, I think you bring appreciation that all of what we do ultimately is about the young men and women who wear the uniform, that really are in harm's way. For what you do for them, I thank you.

Chairman LEVIN. Thank you, Senator Reed.

Senator Wicker.

Senator WICKER. Thank you, Mr. Chairman.

Thanks to both of our witnesses today. Let me try to be brief.

General Selva, I want to talk about moving C–130Js from Keesler Air Force Base. But let me say that DOD wants to do another base realignment and closure (BRAC) round, and often we hear Defense officials say it's not going to be like the 2005 BRAC round. They say: Our days of spending lots of money just moving things around that won't result in financial savings, those days are over. Yet with the Air Force plans to shut down the 815th Airlift Squadron and their Active Duty partners, the 345th Airlift Squadron, and move the squadron of C–130J aircraft away from Keesler Air Force Base, it seems to me the reasons have never been fully explained.

The official announcement came yesterday. I have a news report from WLOX of Biloxi, MS, which says Keesler Air Force Base will lose 10 aircraft from the 403rd Wing under proposed defense cuts presented to Congress on Monday. The Air Force Reserve Command plans to transfer the 10 C–130J aircraft to the newly reactivated—newly reactivated—913th Airlift Group in Little Rock.

First, I'm willing to work with the Air Force in making overall savings. Every Senator is going to defend our own bases. But if this is going to help the greater good, count me in to be your teammate here.

But first these aircraft were going to go to Dobbins in Georgia. The Air Force abandoned that, and then they were going to send them to Pope Field to the 44th Airlift Wing in North Carolina. Now that wing's going to be deactivated, and we're newly reactivating

an airlift group at Little Rock and sending these C–130Js from Keesler to Little Rock Air Force Base, to this newly reactivated group.

The taxpayers have spent millions of dollars to provide Keesler Air Force Base with state of the art modern hangars and facilities. As a matter of fact, Keesler has enough space to house two squadrons. Yet the Air Force continues to propose to spend millions of dollars to move these aircraft away.

I just want you to help us understand at the committee level the reason for this. Of course, the move would also cause serious disruptions to the unit's personnel and their families, and that happens every time there's a move. I just want to ask you three direct questions, General:

How much will this move cost?

General SELVA. Senator, my understanding is that the move itself is cost-neutral to Little Rock. The savings are on the order of 600 manpower billets across the Air Force Reserve specifically as the Reserves looked at this decision, which equates to about $100 million across the Future Years Defense Program (FYDP) for savings.

Senator WICKER. Okay. Is there going to be any military construction (MILCON) needed at Little Rock to accomplish this move?

General SELVA. Not to my knowledge.

Senator WICKER. Now, I want you to supply me a statement then on the record, not to your knowledge. I want you to be able to look us in the eye on this committee, General, and assure us that not $1 of MILCON is going to be needed to accomplish this move.

General SELVA. Sir, I'll look into the costs of the move from the specifics of what might be required at Little Rock that wouldn't either be required at Pope or any other location where we would base that unit.

Senator WICKER. It is your testimony that moving these 10 aircraft from a base where there's already modern hangars and facilities to a new base is actually going to save enough money to offset the cost of making this move?

General SELVA. Senator, based on the consultations I've had with the Air Force Reserve Command in their making this decision and recommending it to the Air Force, my understanding is that they will save upwards of 600 manpower billets and that will save us $100 million across the FYDP, and that it's a reasonable thing to do.

Senator WICKER. I want you to get back to us with the specific numbers there.

[The information referred to follows:]

Proposed C–130 fleet reductions in the fiscal year 2015 President's budget, including deactivation of Air Force Reserve Command's 440th Airlift Wing at Pope Army Air Field and Air Force Reserve Command's consolidation at Little Rock Air Force Base from 15 C–130Hs to 10 C–130Js, combined with the existing infrastructure at Little Rock Air Force Base results in no additional MILCON needed to integrate Air Force Reserve Command's 10 C–130J aircraft at Little Rock Air Force Base.

Senator WICKER. Let me just follow up on Senator Manchin's question about equipment being left in Afghanistan. I think your

testimony was that you really weren't in a position to comment about equipment left in Iraq, is that correct?

General SELVA. Sir, I'm not in a position to testify about the details of the equipment left in Iraq because I wasn't in that decision process.

Senator WICKER. Okay, but you are going to get back with the committee and with Senator Manchin on some follow-up answers regarding equipment being left in Afghanistan, is that correct?

General SELVA. Senator, the decisions on equipment left in Afghanistan will be up to General Austin in CENTCOM and General Dunford in ISAF, as well as our DOD leadership. The comment I made to Senator Manchin was there is some equipment that would normally be left in Afghanistan as a result of the value of the equipment, the residual value of the equipment, being less than the transportation costs in having to bring it home.

Senator WICKER. Are you going to be able to get back to the committee about the factors there or do you suggest that Senator Manchin and I look elsewhere?

General SELVA. Sir, I would have to consult with General Austin and General Dunford——

Senator WICKER. It's a question for another command?

General SELVA. Yes, sir.

Senator WICKER. Okay. But it goes without saying—number one, we're going to leave friends there. Hopefully we're going to leave a follow-on force.

General SELVA. Yes, sir.

Senator WICKER. Hopefully, we're going to try to continue to be successful in Afghanistan. There are some forces that are going to need this equipment.

Second, there would be a cost to the taxpayers of transporting some of this equipment back that's not going to be necessary for us to be successful in the long haul, and it would make no sense to spend the money to bring it back if it's going to cost more. Would that be a fair statement?

General SELVA. That's correct, sir.

Senator WICKER. Thank you very much. Good luck to both of you.

Chairman LEVIN. Thank you, Senator Wicker.

Let me interrupt just for one second. The first vote has now begun. I believe it's the first of four that are scheduled. After Senator Vitter, I think that Senator Kaine is coming back, and if there are no other Senators I'm then going to ask Senator Kaine, who is coming back I understand, to close off, unless Senator Inhofe has a different plan. Thank you.

Senator Vitter.

Senator VITTER. Thank you, Mr. Chairman, and thanks to our witnesses for all of your service and for being here.

Admiral Rogers, do you think that CYBERCOM has the necessary supporting policies and authorities and relationships and the will to act? Are all of those in place, and if you would supplement any of those what additional authorities or policies would you like to see?

Admiral ROGERS. In general, my immediate answer would be yes. I think as I've already indicated, that the things I think we need to continue to work on are this idea of deterrence, this idea of de-

veloping norms within the cyber arena. That's going to be much broader than just CYBERCOM, but clearly CYBERCOM I believe is part of that dialogue.

Senator VITTER. But within CYBERCOM, do you have the authorities and the policies you need to do all of that effectively?

Admiral ROGERS. Yes, sir.

If I could, and if I am confirmed and my experience leads me to believe otherwise in actually executing the mission, I will come back.

Senator VITTER. Okay. In your statement you said, "The level of expertise required to conduct potentially damaging operations has steadily lowered, enabling less capable actors to achieve some level of effect." How does this impact our allies and foreign partners and our ability to work with them?

Admiral ROGERS. I think it increases the level of risk for all of us, for all of our partners.

Senator VITTER. Is it in particular a problem when we have allies and partners with less capable defenses than we do, and how do you handle that?

Admiral ROGERS. Yes, sir, and I think one of the ways we handle that is through strong, broad partnerships. We have a strong dialogue in the cyber arena now with many of our allies and partners. We need to continue to build on that.

Senator VITTER. I know the Pentagon, for instance, wants more NATO members to have more access to unmanned aircraft. Are there particular issues or threats or vulnerabilities related to that, given these advanced opportunities for our enemies to have an effect?

Admiral ROGERS. Yes, sir, there clearly is a risk there.

Senator VITTER. How do we mitigate and hedge against that risk?

Admiral ROGERS. I think we ask ourselves what can we do to try to mitigate that risk, whether it's changes to the physical systems on those aircraft themselves, whether it's asking ourselves what kind of tactics, techniques, and procedures are we doing that can help maximize our attempts to mitigate that risk.

Senator VITTER. Are those risks ever such that, with regard to particular systems, we would change our mind in terms of a transfer to an ally?

Admiral ROGERS. Clearly it would be on a case-by-case basis. None that I'm currently aware of.

Senator VITTER. Okay. Last week the press reported that Russia had used cyber-attacks against Ukrainian telecommunications, to hamper Ukrainian leadership's ability to access that. Do you agree that Russia has very sophisticated cyber capabilities, and if they use them that could impart considerable damage to Ukraine's critical infrastructure?

Admiral ROGERS. Yes, sir, I would agree with both of those statements.

Senator VITTER. I want to move to Guard and Reserve, Admiral Rogers. A lot of us are interested in better integrating and using, leveraging, Guard and Reserve capabilities. Clearly it's a long-term trend that the Guard and Reserve are much more in the middle of any effort, any fight we have. What specifically is CYBERCOM

doing to ensure that the Guard and Reserve components are being fully utilized and maximized?

Admiral ROGERS. First, CYBERCOM is part of that broader departmental discussion, that review that's ongoing right now, that is scheduled to be finished by July, that's designed to take a look at the mission analysis associated with asking ourselves just what kind of Reserve capability in the cyber arena do we need, how do we bring it to bear, how do we structure the Reserve component to maximize its effectiveness and its part in this mission.

In addition, CYBERCOM currently has an ongoing series of exercises designed to exercise with Guard units in the cyber arena. CYBERCOM also has an ongoing dialogue and is part of a broader dialogue with governors and the adjutant generals as we work our way forward to figure out what's the best way to maximize that capability, and we have to maximize that capability.

Senator VITTER. I would underscore and encourage that with regard to CYBERCOM in particular. As I hope you know, there's particular language in the last defense authorization bill requiring maximization of that with regard to the Guard and Reserve. I would really commend that to your focus and attention.

A final question. I think some of your comments have gone to the fact that appropriate leadership needs to make the case more fully and publicly and persuasively for the use of important authorities that do exist and lay that out in layman's terms, if you will, why it's important. In that spirit, can you talk to a capability that has been fairly hotly debated, which is the use of geographic information regarding cellphones?

Admiral ROGERS. To be honest, sir, it's not an issue I have yet delved deeply into. It's one of those things I need to get specificly smarter on to be prepared to discuss very publicly. I think that's an important part of that public discussion.

Senator VITTER. If you could look at that and maybe supplement the record in writing with regard to your thoughts on that, I would appreciate it.

Admiral ROGERS. Yes, sir.

[The information referred to follows:]

I appreciate that there has been some concern raised about whether the National Security Agency (NSA) would seek to obtain Cell Site Location Information (CSLI) under section 215 of the Patriot Act. CSLI provides identifying information for the cell tower used initially to place or receive the call. While CSLI identifies the tower, it does not reveal the precise location of the mobile device used to place or receive the call. As detailed in several declassified court orders by the Foreign Intelligence Surveillance Court (FISC), NSA is not authorized to obtain CSLI as part of the section 215 Telephony Metadata Program. Accordingly, should NSA seek to obtain CSLI under section 215 at a future point in time it would need to obtain the approval of the FISC. It is important to note, however, that CSLI is potentially useful intelligence information in many other contexts, such as counterterrorism investigations and in support of U.S. military and intelligence operations abroad. For example, it could well be that knowing the general location where a terrorist was located or where an individual in contact with a terrorist was located when a call was made would be a key piece of information to those responsible for protecting the Homeland.

Senator VITTER. That's all I have. Thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator Vitter.

Senator Kaine, when you're done, we're in the middle of a vote now—you have voted on this one, have you?

Senator KAINE. I have, Mr. Chairman.

Chairman LEVIN. If you could then turn it over to whoever is here next in line, I'd appreciate it.

Senator KAINE. I will. Thank you, Mr. Chairman.

Thanks to the witnesses for your service and for your testimony today. My questions will be primarily for Admiral Rogers.

I have a little bit of an unorthodox view of some of these challenges about NSA programs. Many of my colleagues talk about these programs as if the solution to controversies is fixing the programs themselves, and I actually think the bigger challenge is many of these programs are being carried out pursuant to a vaguely defined war or conflict.

Admiral Rogers, twice during your testimony today I think your testimony has at the vague notion of what we are, in fact, in. You indicated that you thought Edward Snowden's revelations were wrong and that they cost American lives, but you hesitated about whether to use the word traitor to describe Edward Snowden. When you were asked by Senator Graham whether we were at war, you said we're in a hostility or disagreement. But then there was a misunderstanding in terms of what he was asking. You thought he was asking about a cyber-war in particular; you understood that we're in a war on terror.

My concern is we are carrying out a whole series of military actions and intelligence programs that are being done pursuant to an authorization for use of military force that was done on September 14, 2001, that has no temporal limitation, that has no geographic limitation, and that has been defined by both the Bush and Obama administrations to extend to taking action not only against those who planned the September 11 attack, but against associated forces. That language does not appear in the authorization, but it has been the administrations', both administrations', decision about what that authorization means.

We are currently in a war, but the war does not have a geographic limitation. It does not have any kind of a temporal limitation. It doesn't have an expiration date. This committee held a hearing on the authorization for use of military force in May. I asked Obama administration witnesses when does this war end, and they said: We're not sure; it could be 25 or 30 years.

I asked Obama administration witnesses: If someone who is born in 2020 and when they're 15 years old in 2035 joins an organization that is associated with al Qaeda that only popped up then, that has no designs against the United States, does the authorization allow us to take military action against that individual or that group? The answer was yes.

There is no reform that we're going to be able to make to any of these NSA programs that I think will answer the questions of our citizens or civilians if our intelligence-gathering operation is done in a significant way pursuant to an open-ended military authorization. The questions that you received about the dual-hatted nature of your job—you're part of a military command that is executing an authorization that has no limitation whatsoever for all practical purposes, and you're also in an NSA position where you're gathering intelligence.

I feel like the challenge about limiting these NSA programs or trying to find the right balance between fighting terrorism, stopping evil, and protecting citizens' rights—we can do anything we want within the four corners of the programs. If we do not as a Congress revisit the 2001 authorization and try to put some sense of definition and scope to it—open-ended, it could be a war for another 25 or 30 years—we'll continue to have witnesses, sharp witnesses who are very talented, who will come before us and will have difficulty describing exactly what we're in the middle of because the primary job of Congress is to give some definition at the front end in terms of what the mission is. It's the military and the Commander in Chief that have to execute the mission.

But Congress has given no definition of what it is we are doing at this point, and we will always have controversies in my opinion going forward.

Now, Admiral Rogers, in your advance policy questions you were asked about what constitutes use of force in cyber space in relation to the War Powers Act, the exercise of the right of self-defense under the United Nations (U.N.) Charter, and also the triggering of collective defense obligations. I'd like if you could just elaborate a little bit on that answer today, use of force in cyber space and how in your view that triggers either the war powers or other obligations that the United States has.

Admiral ROGERS. I'd be first to admit, I apologize, of the 120 questions I was asked, I don't remember word for word the specifics. Please, accept my apologies.

Senator KAINE. Yes, indeed. What are unique challenges in defining "war" in cyber space, what war is, what hostilities are, what military action is?

Admiral ROGERS. Clearly, from a policy perspective we are still trying to work our way through those issues. The tenets I think that are applicable here are the fact that, whatever we do within the cyber arena, international law will pertain; that if we find ourselves getting to a point where we believe that cyber is taking us down an armed conflict scenario, that the rules and the law of armed conflict will pertain every bit as much in this domain as it does in any other.

I don't think cyber is inherently different in that regard. I think those sets of procedures, those sets of policies and law, as a Nation have stood us in good stead. I think they represent a good point of departure for us.

Senator KAINE. The phrase you used I think is an interesting one: If we believe that cyber activity is taking us down the path to armed conflict, then international law would apply. Would it be your view then that pure cyber war—somebody wipes out our grid and then we think about taking activity to respond—is that not war? It could have huge effect on human life. It could have huge effect on the economies of the two nations. Is that not war unless it then leads to armed conflict?

Admiral ROGERS. No, certainly I believe that an offensive, destructive act that has significant impact for us, I believe now we're starting to get on the boundaries of is that an act of war. Now, everything varies on a case by case basis and I'm always concerned about broad general statements.

Senator KAINE. Right. It is just that question. We do have some important definitional work to do. The absence of a cyber-bill makes this all harder for all of us.

Let's switch topics. Yesterday I visited Northern Virginia Community College and was fortunate to be there at a time where there was a meeting of the DC-based organization CyberWatch, which was set up a number of years ago to help colleges, community colleges, and the private sector, coordinate what they think are the skills that our cyber professionals need. It's a work force organization.

I was interested that someone from DOD is not commonly around that table and I might want to follow up separately to suggest that that would be a good avenue for participation.

There has been testimony—General Alexander was here last week—on the need for 133 cyber mission teams managed by 6,000 highly trained personnel by 2016. As the leader of CYBERCOM, what will be your approach on these recruiting and training issues? Because, first, the need is intense; and second, the competition from the private sector is also very intense for people with this skill set. What will your approach be to staffing out this important mission?

Admiral ROGERS. First, each of the Services continues to pay particular attention to this in their responsibilities to man, train, and equip the cyber force. As the Navy individual right now, to be honest, on the uniformed side our experience has exceeded our expectations. We have been able to recruit quality individuals and retain them. It's something I, in my current duties, continue to pay close attention to: What are the indicators that would suggest that potentially that is changing?

In some ways, the civilian side I think represents an even potentially greater challenge. I think we need to look at incentives, whether that be pay, whether that be the ability to focus these individuals in particular areas for extended periods of time, in ways that traditionally we don't do now. I think we'll need to look at all of that.

Senator KAINE. When you say the civilian side, you mean to do the work of CYBERCOM it takes a real balance of Service branch personnel, but also DOD civilians.

Admiral ROGERS. Yes, sir.

Senator KAINE. There has to be a good mixture.

Admiral ROGERS. Yes, sir.

Senator KAINE [presiding]. My time is up and all who are here for first rounds of questions are done. Is there a second round of questions? Ranking Member Inhofe?

Senator INHOFE. Yes, Mr. Chairman. If you'd like to go ahead and continue, you could. I know that Senator Cruz is coming back, although you were involved, starting to talk about something that I unsuccessfully was trying to get at during my time, and that is this threat. I just fail to see that there's a major difference between someone who is attacking us, depending on what kind of weapon they're using, and this weapon of cyber attack.

Let me ask you, Admiral Rogers, do you believe we're deterring or dissuading our adversaries in cyber space and out? Do you think we're deterring them?

Admiral ROGERS. Not to the extent we need to, sir, no.

Senator INHOFE. Do you know what cyber deterrence looks like?

Admiral ROGERS. No, sir. We're still working our way——

Senator INHOFE. That's the problem. There's not a lot of the public out there that is aware of the significance of what's going on. When I talk to people out there about what Iran's capabilities are, what they're going to be next year. We talk about a weapon, we talk about a delivery system, they understand that, but not cyber attack. I look at this and I just think that the Senator from Virginia was really onto something. A war is a war, and I think we're going to have to elevate the threat that we're talking about in this committee and you'll be dealing with, both of you are going to be dealing with, to the level of a military threat, because I think most people are not really aware of that.

General Selva, DOD uses rail primarily for large training exercises and deployments. It also depends on the rail industry to be ready to meet DOD's surge requirements. What is your assessment of the rail industry to support DOD's requirements?

General SELVA. Senator, I'm not in a position as the Air Mobility Command Commander to give you a definitive answer other than to say that, having consulted with TRANSCOM, the recent work that's been done to look at the number of available rail cars and the status of the rail infrastructure in the Nation is in the hands of the TRANSCOM Evaluation and Assessments Division. I'll be happy to take a look into that data once I have an opportunity to do that if confirmed. But it's so far out of the area of my expertise right now, it wouldn't be appropriate for me to give you a definitive comment.

Senator INHOFE. Admiral Rogers, I mentioned earlier that I have gotten to know the outgoing man in charge, General Alexander, quite well, and I've had a chance to talk to him some time ago, early on. I think he's really done an excellent job and he has informed me that you have the type of background that is going to be able to do the same thing. I would just hope that we could work together in getting this, raising this in the eyes and the views of the public so that people understand how real the threat is out there. I look forward to working with you.

Senator KAINE. Thank you, Ranking Member Inhofe.

Senator Cruz.

Senator CRUZ. Thank you, Senator Kaine.

General, Admiral, thank you both for being here. Thank you both for your long and distinguished service to our Nation.

Admiral, I'd like to talk some about the NSA's policies. I have long expressed concerns about the NSA's policies on really two fronts: one, an overbroad intrusion into the privacy rights of law-abiding citizens; and two, a pattern of not focusing sufficiently on bad actors and not collecting the information, the intelligence needed to prevent terrorist acts. It seems to me the focus overall of our intelligence and defense community and law enforcement community is directed far too much at law-abiding citizens and far too little at individualized bad actors. I'd like to ask you questions on both fronts.

Starting out with the citizenry at large: As you're aware, President Obama's Review Group on Intelligence and Communications

Technology has said that the bulk metadata collected by the NSA should be held by a third party, and the Privacy and Civil Liberties Oversight Board has recommended ending bulk metadata collection altogether. Do you agree with either of these proposals?

Admiral ROGERS. In terms of pulling the data from the NSA, yes, I believe that there is a standard that we can work toward that would enable us to do that while still meeting the requirements of generating the intelligence we need and ensuring the protection of U.S. citizens.

Sir, would you mind repeating the second portion?

Senator CRUZ. The second portion was that the Privacy and Civil Liberties Oversight Board recommended ending bulk metadata collection altogether, and I was asking if you agree with that recommendation.

Admiral ROGERS. No, sir, I would not. I believe we can still do this in a way that ensure the protection of our citizens while also providing us insights that generate value.

Senator CRUZ. But you believe that the information should not be held by the U.S. Government, is that correct?

Admiral ROGERS. I support the President's decision to shift that from the NSA.

Senator CRUZ. If confirmed, what would be a timetable for implementing that reform?

Admiral ROGERS. To be honest, sir, I don't know. I'm just not smart enough yet about the particulars. It'll be driven by the solution that we come up with. That dialogue is ongoing right now. I haven't been a part of that as a nominee.

Senator CRUZ. Will you commit, if confirmed, to working with members of this committee to implement it expeditiously?

Admiral ROGERS. Yes, sir.

Senator CRUZ. I want to ask more generally. The Fourth Amendment protects the privacy of law-abiding Americans. What is your view of the appropriate limitations on the ability of the Government to search through phone or email communications of law-abiding citizens not accused or under suspicion of any wrongdoing?

Admiral ROGERS. I believe such searches should not be done without a corresponding legal framework for their execution.

Senator CRUZ. Does that framework in your judgment require individualized suspicion?

Admiral ROGERS. I think it varies by the specifics of the threat that we're talking about, which is one reason why the metadata approach I think was taken to try to address that, to deal with no content, no names, no geographic locations, to try to strike that balance, if you will.

Senator CRUZ. Would you agree that for the Government to intercept content from telephones or emails requires under the Fourth Amendment individualized suspicion and some form of judicial oversight?

Admiral ROGERS. I don't know that I would make a blanket statement. Again, sir, I apologize; I am not a lawyer and you're asking me about the specifics of the law and it's just not an area of my expertise.

Senator CRUZ. I would ask after this hearing if you would follow up and answer that question in writing, and you can certainly con-

sult with counsel. But the relevance of the Fourth Amendment in terms of how you would implement the policies at the NSA I think is a question of great interest to a great many citizens, and the Government collecting metadata or even more so the content of communications between law-abiding citizens is an issue that the Constitution I believe speaks very directly to. I would appreciate your expanded answer in writing after this hearing.

[The information referred to follows:]

Admiral ROGERS. It is certainly the case that Americans are protected by the Fourth Amendment from unreasonable searches and I am fully committed to protecting this and all other rights of Americans. As to the requirements of the Fourth Amendment for the Government to intercept content from telephone calls or emails, I understand that this legal doctrine is the subject of numerous Supreme Court decisions and that those requirements would depend on the particular facts and circumstances of a given situation. Under the Foreign Intelligence Surveillance Act, absent limited exceptions such as an emergency, the National Security Agency may not target any unconsenting U.S. person anywhere in the world under circumstances in which the U.S. person would enjoy a reasonable expectation of privacy without an individualized determination of probable cause by a Federal judge that the target is a foreign power or agent of a foreign power.

Senator CRUZ. I'd like to shift to the other side, to the concern that I have that we are devoting far too many resources looking at law-abiding citizens and far too few resources looking at the bad guys. With regard, for example, to the Boston bombing, the Tsarnaev brothers, we had been notified by Russia that in their judgment they were having communications and may be radical Islamic terrorists. The elder Tsarnaev brother posted and advertised his desire for jihad on YouTube, not exactly a secure, hidden communication, but publicly for the world to see.

Yet, even though we knew this individual or had reason to know this individual was a radical Islamic terrorist, and even though he was publicly proclaiming his desire for jihad, we failed to prevent that tragic bombing in Boston. I'd like to ask you, why do you think that was and what can we do to correct it so we don't fail to prevent the next Boston bombing?

Admiral ROGERS. The reality is, sir, I don't know the specifics of the Boston bombing. It's not an element of my current duties and it's not something I have express direct knowledge of. I think to comment knowingly I would need that kind of knowledge.

Senator CRUZ. A second example deals with Major Nidal Hassan and the Fort Hood murders. In that instance, Hassan had traded some 18 emails with radical Islamic cleric Anwar al-Awlaki, a known terrorist leader who was a spiritual adviser of the September 11 bombers. This is not some extraneous person. This is someone known to be a serious threat to this country, and a major in the military is communicating repeatedly by email with him.

Despite all of our surveillance capabilities, we failed to prevent that horrific terrorist attack at Fort Hood that claimed the lives of 14 innocents. In your judgment, why was that? What could we have done better to prevent that?

Admiral ROGERS. To be honest, I answered that question to Senator Graham.

Senator CRUZ. Let me suggest more broadly on both of these that it would be a far better allocation of resources in the NSA and in our efforts to prevent terrorism generally if much more resources were directed to targeting those who we have reason to know are

dangerous, we have reason to know are or may be radical Islamic terrorists, and less resources were devoted and less energy was devoted to broader interception and surveillance of the law-abiding citizenry.

It has struck me for some time that the priorities have been backwards and we ought to be targeting the bad guys and protecting innocents from terrorist attacks and at the same time respecting the constitutional rights of every American.

Thank you, Admiral. Thank you, General.

Senator KAINE. Thank you, Senator Cruz.

Senator Inhofe, any additional questions for a second round of questioning?

Senator INHOFE. No.

Senator KAINE. Seeing none, I thank the witnesses for your appearance today and for your patience as we were going back and forth to vote. We appreciate your service and this hearing is adjourned.

[Whereupon, at 12:00 p.m., the committee adjourned.]

[Prepared questions submitted to Gen. Paul J. Selva, USAF, by Chairman Levin prior to the hearing with answers supplied follow:]

QUESTIONS AND RESPONSES

DEFENSE REFORMS

Question. The Goldwater-Nichols Department of Defense Reorganization Act of 1986 and the Special Operations reforms have strengthened the warfighting readiness of our Armed Forces. They have enhanced civilian control and clearly delineated the operational chain of command and the responsibilities and authorities of the combatant commanders, and the role of the Chairman of the Joint Chiefs of Staff. They have also clarified the responsibility of the Military Departments to recruit, organize, train, equip, and maintain forces for assignment to the combatant commanders.

Do you see the need for modifications of any Goldwater-Nichols Act provisions?

Answer. I believe Goldwater-Nichols has transformed the Department of Defense (DOD) for the better and it has led to an unprecedented level of cooperation and understanding between the Services. Over the last 28 years, DOD and the military have fully embraced joint, interdependent operations. Having the opportunity to serve in multiple joint tours and now as Commander of Air Mobility Command, I have seen first-hand how we continue to improve our joint capabilities, ultimately producing a more effective means to grow the officers who are capable of leading our soldiers, sailors, airmen, and marines as a joint force.

Question. If so, what areas do you believe might be appropriate to address in these modifications?

Answer. I have no suggestions for altering Goldwater-Nichols at present, but I do recognize the need to continuously review and improve the framework in which DOD operates. If confirmed, I will work with Congress, the Secretary of Defense and other senior leaders of our military to ensure Goldwater-Nichols continues to meet the needs of our Armed Forces and champion any changes to the legislation that might become necessary.

DUTIES

Question. What is your understanding of the duties and functions of the Commander, U.S. Transportation Command (TRANSCOM)?

Answer. The mission of the Commander, TRANSCOM is to provide air, land and sea transportation for DOD, in peace, crisis, and war. TRANSCOM relies on three Component Commands—Air Mobility Command (AMC), Military Sealift Command (MSC), and the Military Surface Deployment and Distribution Command (SDDC)—to accomplish this mission. The Commander has been assigned numerous responsibilities in the Unified Command Plan (UCP) to include the Distribution Process Owner (DPO) mission to improve the worldwide DOD distribution system; DOD single manager for global patient movement; Global Distribution Synchronizer (GDS)

mission for synchronizing Phase 0 distribution operations; and facilitating the rapid establishment of joint force headquarters for combatant commanders through its subordinate command, Joint Enabling Capabilities Command. The TRANSCOM Team utilizes a blend of Active and Reserve Forces, civilian employees, and commercial industry partners to meet the command mission in support of a full range of military operations.

Question. What background and experience do you possess that you believe qualifies you to perform these duties?

Answer. Throughout my military career, I have had the opportunity to be in positions that have prepared me, if confirmed, to perform the duties as the Commander of TRANSCOM.

As the Assistant to the Chairman, Joint Chiefs of Staff, I had the opportunity to serve as an advisor to the Secretary of State and senior State Department leaders. In that capacity I worked directly with senior diplomats strengthening our relationship with allies, partners and friends, and building partnerships with foreign governments and international and non-governmental organizations.

As a previous Director of Operations in TRANSCOM, I directed and synchronized the Defense Transportation System with national distribution processes to meet national security objectives. During my tenure I was responsible for day-to-day operations of the transportation and logistics networks that supported our forces engaged in combat in both Iraq and Afghanistan and supported humanitarian relief and disaster response operations at home and abroad.

Finally, in my current capacity as Commander, Air Mobility Command, the Air Component of TRANSCOM, I command over 130,000 airmen from across our Air Force, Active, Reserve, and Air National Guard who provide worldwide cargo and passenger delivery, aerial refueling, special air mission and aeromedical evacuation. This includes the crucial role of humanitarian assistance and disaster relief to victims of natural disasters both at home and around the world.

Question. Do you believe that there are any steps that you need to take to enhance your expertise to perform the duties of the Commander, TRANSCOM?

Answer. As a previous Director of Operations for TRANSCOM and as the current commander of one of TRANSCOM's Service components, I am aware of the command's global responsibilities. If confirmed, I will personally engage with all of TRANSCOM's component commands, DOD agencies, and commercial partners to ensure I fully understand the scope of the issues they face in order to execute this critical duty.

RELATIONSHIPS

Question. Section 162(b) of title 10, U.S.C., provides that the chain of command runs from the President to the Secretary of Defense and from the Secretary of Defense to the combatant commands. Other sections of law and traditional practice, however, establish important relationships outside the chain of command. Please describe your understanding of the relationship of the Commander, U.S. Transportation Command to the following offices:

The Deputy Secretary of Defense.

Answer. The Deputy Secretary of Defense has full power and authority to act for the Secretary of Defense when serving as his designated representative in the Secretary's absence. As such, the Commander TRANSCOM will report to and through the Deputy Secretary when serving in that capacity. The Deputy Secretary also serves as the Chief Management Officer of DOD to optimize the business environment across the Defense enterprise. TRANSCOM supports such optimization to improve our support to the other combatant commands, at best value to the Nation.

Question. The Under Secretaries of Defense.

Answer. Under Secretaries of Defense coordinate and exchange information with DOD components, including combatant commands, which have collateral or related functions. In practice, this coordination and exchange is normally routed through the Chairman of the Joint Chiefs of Staff. In addition, as the DPO, the TRANSCOM commander receives oversight from the Under Secretary of Defense for Acquisition, Technology, and Logistics in his role as the Defense Logistics Executive via the Defense Logistics Board. If confirmed as a combatant commander, I will act accordingly.

Question. The Chairman of the Joint Chiefs of Staff.

Answer. The Chairman is established by title 10 as the principal military advisor to the President, the National Security Council, the Homeland Security Council, and Secretary of Defense. The Chairman serves as an advisor, and is not, according to the law, in the chain of command, which runs from the President through the Secretary to each combatant commander. The President normally directs communica-

tions between himself and the Secretary of Defense to the combatant commanders via the Chairman of the Joint Chief of Staff. This keeps the Chairman fully involved and allows the Chairman to execute his other legal responsibilities. A key responsibility of the Chairman is to speak for the combatant commanders, especially on operational requirements. If confirmed, I will keep the Chairman and the Secretary of Defense promptly informed on matters for which I would be personally accountable.

Question. The Vice Chairman of the Joint Chiefs of Staff.

Answer. Although the Vice Chairman does not fall within the combatant command chain of command, he is delegated full power and authority to act for the Chairman in the Chairman's absence. If confirmed as a combatant commander, I will keep the Chairman informed, but if the Vice Chairman is representing the Chairman I will keep him informed as I would the Chairman.

Question. The Director of the Joint Staff.

Answer. The Director of the Joint Staff assists the Chairman in managing the Joint Staff. The Director of the Joint Staff does not fall within the combatant commander's chain of command. However, he enables important decisions to be made as the combatant commander's staff interacts with the Joint Staff. The Director is also a key interface with Office of the Secretary of Defense principles and interagency leadership, and can assist combatant commanders working issues below the Chairman's level.

Question. The Secretaries of the Military Departments.

Answer. Each Service Secretary is responsible for equipping, training, maintaining, and administering forces in the Secretary's Service. Close coordination with each Service Secretary is required to ensure that there is no infringement upon the lawful responsibilities held by a Service Secretary.

Question. The Chiefs of Staff of the Services.

Answer. The Chiefs of Staff of the Services organize, train, and equip their respective forces. No combatant commander can ensure preparedness of his assigned forces without the full cooperation and support of the Service Chiefs and their respective Reserve components. As members of the Joint Chiefs of Staff, the Service Chiefs have a lawful obligation to provide military advice. The experience and judgment the Service Chiefs provide is an invaluable resource for every combatant commander. If confirmed, as Commander, TRANSCOM, I will pursue an open dialogue with the Service Chiefs and the Commandant of the U.S. Coast Guard.

Question. The other combatant commanders.

Answer. Each combatant commander is assigned specific responsibilities in the Unified Command Plan. Given the complexity of today's security environment, it is essential that all the combatant commanders work together to execute U.S. national security policy. If confirmed, I will maintain open dialogue with the other combatant commanders to foster trust and build mutual support.

MAJOR CHALLENGES AND PRIORITIES

Question. In your view, what are the major challenges confronting the next Commander, TRANSCOM?

Answer. TRANSCOM currently has the capability to meet all surge requirements, however, long-term budget uncertainty may erode this key, asymmetric military and logistics advantage. TRANSCOM is focused on providing logistics and transportation solutions and increasing efficiencies for all its customers but if the future budgets are not addressed, its readiness, particularly the readiness of commercial partners, could be negatively impacted. Maintaining the readiness of our organic lift and sustaining the readiness of our commercial partners in an uncertain budget environment will present significant challenges to our ability to respond to crisis or conflict.

The talent and skill of the men and women that make up TRANSCOM and its component commands is the foundation of the command's success. I take very seriously the challenge and responsibility as a commander to be the champion for their readiness and to keep the entire team prepared to respond to the needs of the Nation. If confirmed, I would take an active role in preserving and enhancing the quality and expertise of TRANSCOM's personnel resources and will actively address the demand to maintain the readiness of the transportation and distribution networks to respond to crisis or conflict.

Question. If confirmed, what plans do you have for addressing these challenges?

Answer. If confirmed, I will work with my fellow combatant commanders to assess risks and develop mitigation strategies to ensure we can meet steady state and surge requirements. I will work to improve TRANSCOM's global, end-to-end ability to deliver to the point of need in the most cost-effective way possible—projecting American influence and power when and where our national interests dictate. To

do this, I will work with TRANSCOM's commercial partners and the interagency to continue to build and maintain capacity and continue TRANSCOM's efforts around the world to secure diplomatic and physical accesses to ground and airspace infrastructure for logistics. I will also leverage ongoing multi-modal efforts to optimize our operations to support the warfighter while improving the performance and efficiency of the joint deployment and distribution enterprise.

Question. If confirmed, what broad priorities would you establish?

Answer. If confirmed, my main priorities will be to support the warfighter and preserve readiness to meet national objectives. Always mindful of our obligation to make the most of our existing resources, I will continue process improvement and enterprise synchronization efforts through relationships within the Department, across the U.S. Government, and with commercial and international partners.

Question. What do you consider to be the most serious problems in the performance of the functions of the Commander, TRANSCOM?

Answer. In a resource constrained environment, the most significant area I would focus on would be improving the coordination and synchronization of the entire Joint Deployment and Distribution Enterprise—a vast network of organizations both in and out of DOD that relies heavily on commercial partnerships with industry. TRANSCOM has made great strides in improving the economies and efficiencies toward this end, and if confirmed, I will continue this work by aligning enterprise responsibilities commensurate with assigned authorities and available resources; improving our ability to rapidly build strategic distribution networks; and, institutionalizing best practices and lessons learned during more than a decade of war.

Question. If confirmed, what management actions and timelines would you establish to address these problems?

Answer. If confirmed, I will work early to deepen strategic and personal relationships with fellow combatant commanders, TRANSCOM's components, commercial and international partners, interagency leaders and with Members of Congress. We will be challenged with difficult decisions in the near future; however, we must balance costs and benefits, matching our actions to available resources in the near term and adapting our efforts for greater economies and efficiencies in the long term.

EXPERIENCE IN MANAGING LOGISTICS OPERATIONS

Question. You have served as the Commander of the Air Mobility Command.

What steps do you believe you need to take to achieve a more complete understating of the logistics operations of the other component commands of the TRANSCOM?

Answer. Fortunately, as a previous Director of Operations for TRANSCOM and as the current commander of one of TRANSCOM's Service components, I have an in-depth knowledge of the missions, roles and responsibilities of all facets of the TRANSCOM team. If confirmed, I will make it a priority to offer continued engagement with the component commanders, DOD agencies, and commercial partners to increase my understanding of the issues they face in order to better execute TRANSCOM's critical worldwide mission.

DISTRIBUTION PROCESS OWNER

Question. In September 2003, following a review of logistics operations, the Secretary of Defense designated the Commander, TRANSCOM, as the Distribution Process Owner (DPO). As the DPO, TRANSCOM was tasked to improve the overall efficiency and interoperability of distribution related activities—deployment, sustainment, and redeployment support during peace and war.

What is your understanding of TRANSCOM's responsibilities as the DPO?

Answer. TRANSCOM, in partnership with the Defense Logistics Agency (DLA), General Services Agency, the Services, and combatant commanders others, is responsible for constantly working to improve the effectiveness and efficiency of the DOD Distribution Network. Working with all the network stakeholders, TRANSCOM must work carefully to optimize the effectiveness and efficiency of the entire military supply chain, from factory to end user.

Question. What is your assessment of the progress has TRANSCOM made in improving the distribution process?

Answer. In the last few years our DPO Strategic Opportunities team has focused on a number of cost avoidance initiatives on both the surface and air side. Through these efforts, we have successfully reduced the amount of containers moving globally through both better utilization and a decrease in the amount of less efficient 20 foot containers used. We applied similar utilization principles to aircraft movements to reduce the overall amount of air lift. Along the same lines, we expanded use of continental United States multi-modal hubs to maximize cheaper surface movements.

Finally, we have developed methods to better manage aircraft fuel usage/purchase which is the single largest expense in aircraft operations.

Question. Do you believe that the current system needs any changes to enhance the ability of TRANSCOM to execute the responsibilities of the DPO?

Answer. I believe TRANSCOM has the necessary authorities to execute the Unified Command Plan designated responsibility of the DPO. If confirmed, I will continue the work underway in TRANSCOM's execution of the DOD Global Campaign Plan for Distribution. TRANSCOM is in its first cycle of this recently approved plan which will identify distribution issues, assess their risks, prioritize these issues and finally pursue issue resolutions. The plan has a built-in annual update to ensure it is still enhancing the Global Distribution Network. The plan sets the stage for successful execution of TRANSCOM's DPO role.

STRATEGIC AIRLIFT

Question. According to DOD, the requirement for organic strategic airlift needed to support wartime requirements has fallen to a level of 275 aircraft.

Do you agree with the plan to reduce the number of strategic airlift to a level of 275 aircraft?

Answer. Yes. The Mobility Capability Assessment (MCA) and the Mobility Requirements Capability Study concluded that in general the mobility capabilities support the strategic objectives in the 2012 National Defense Strategy. While certain scenarios presented some mobility challenges, none precluded achievement of U.S. objectives with accepted timelines and risk.

Question. What is your view of the requirements in peacetime for such organic airlift aircraft?

Answer. In peacetime, the organic airlift force flies to maintain readiness to meet its wartime mission. The organic strategic airlift fleet is able to provide 80–90 aircraft per day to meet the DOD's airlift needs.

Question. Do you believe that the Air Force could, at reasonable costs and within reasonable timeframes, reactivate some portion of the fleet of C–5 aircraft if we discover that 275 strategic airlift aircraft is not sufficient to meet our peacetime and wartime needs?

Answer. Yes. C–5s not retained in service have been placed in the Aerospace Maintenance and Regeneration Center at Davis-Monthan Air Force Base in Arizona, where they can be returned to service if needed.

Question. If we decide that 275 strategic airlift aircraft is insufficient to meet our requirements, should we consider buying more C–17 aircraft?

Answer. The purchase of additional C–17s could be one of several alternatives to consider in an Analysis of Alternatives. This option will be increasingly expensive after the production line is shut down.

NORTHERN DISTRIBUTION NETWORK

Question. The Northern Distribution Network (NDN) has been important in delivering equipment and supplies to Afghanistan, in part to reduce the U.S. reliance on supply routes through Pakistan. Yet significant portions of the NDN go through certain countries, particularly in Central Asia, that have extremely poor track records on human rights and corruption.

What do you see as the major challenges to continued use of the NDN to deliver supplies to Afghanistan or withdraw equipment from Afghanistan as we draw down forces there?

Answer. Sustainment and retrograde cargo volumes have greatly reduced with the reduction of troops in Afghanistan and the increased use of both military and commercial multi-modal operations. Should events in Ukraine strain relationships between the United States and Russia and countries strongly influenced by Russia, access to routes north of the Black Sea both for surface and over-flight movement could be limited. Additional concerns include border crossing and convoy security within the country of Afghanistan which could affect surface movement in and out of the country; if the security situation deteriorates, surface access may become very limited.

The NDN accessed through the Mediterranean and the Caspian remain open and reliable as the countries involved are deeply interested in maintaining routes which will help them build the "New Silk Road" initiative.

Question. To what extent, if any, should concerns about the human rights and corruption records of authoritarian regimes, particularly in Central Asia, be taken into account in using access to supply routes along the NDN?

Answer. The DOD agencies, Department of State (DOS), and geographic combatant commands coordinate closely to develop and maintain NDN routes to ensure an

efficient and effective means of moving warfighter cargo into and out of Afghanistan. Human rights violations as determined by the DOS, and corruption records, should be considered for participation on the NDN.

STRATEGIC SEALIFT

Question. Strategic sealift has always played a significant role in providing support to our forces overseas. Typically, we have seen strategic sealift delivering 95 percent of the equipment transported to overseas contingencies.

An important component of our strategic sealift surge capability is the Ready Reserve Force (RRF). Many of the ships in the RRF are well beyond economic service life and may need to be replaced in the near future.

What plans do you believe would be appropriate for modernizing the RRF?

Answer. The capacity provided by the RRF is critical to TRANSCOM's ability to meet its wartime requirements. In the past, the fleet capacity was increased by using authorities to purchase vessels. The capacity was then maintained using selective Extended Service Life (ESL) programs on vessels where it was appropriate. For the future, we will explore all options to find a recapitalization strategy that is cost effective and minimizes the cost of ownership of the fleet for the long term, to include purchase and ESL where it makes sense.

Question. What will the 2014 Quadrennial Defense Review (QDR) recommend for both airlift and sealift requirements?

Answer. The QDR recommended combat coded inventory (i.e. PMAI) force structure for Air Force in fiscal year 2019 is 211 strategic airlift aircraft (39 C–5, 172 C–17) and 300 tactical aircraft (C–130). The sealift requirements were not defined as main elements in the Navy fiscal year 2019 force structure. If confirmed, I will work with the Navy, U.S. Maritime Administration (MARAD), and MSC to ensure we have adequate organic and commercial sealift capacity in the future. Moreover, I would reiterate the criticality of organic and commercial mobility capability and capacity, including robust sealift and aerial refueling, which remain the foundation of our Nation's ability to project power.

Question. What is your assessment of the effectiveness of the National Defense Sealift Fund (NDSF) to facilitate resourcing sealift?

Answer. Beginning in fiscal year 2015, Navy transferred NDSF funding to other appropriations, preserving the readiness of TRANSCOM's Surge Sealift assets. TRANSCOM supports Navy's effort to be auditable in accordance with Financial Improvement and Audit Readiness standards.

Question. What would be the impact to strategic sealift if the NDSF were closed out and sealift funded out of through other Navy appropriations?

Answer. It is my understanding that this change is an internal Navy funding realignment. Appropriated funds will be used by the Navy for our strategic sealift requirements. TRANSCOM will still have full visibility over these funds.

Question. If you believe the NDSF has worked well, what is your assessment of the potential benefits that could be achieved by establishing a similar or combined airlift-sealift mobility fund to provide resources for both sealift and airlift and promote cost effective tradeoffs?

Answer. TRANSCOM's Transportation Working Capital Fund (TWCF) was established to achieve land, sea and air cost effective tradeoffs while maintaining readiness. If confirmed I would explore options to improve transportation tradeoffs as well as afford better alternatives for readiness.

Question. Are there any initiatives that you would pursue, if confirmed, to modernize or sustain our strategic sealift capability?

Answer. TRANSCOM is currently examining various cost effective options to maintain our organic sealift capacity. If confirmed, I will work with the U.S. Navy, the Maritime Administration and the Office of the Secretary of Defense to implement a cost effective and timely recapitalization strategy to ensure critical vessel capacity is not lost in the organic fleets.

MARITIME SECURITY PROGRAM

Question. Through programs like the Maritime Security Program (MSP), the Voluntary Intermodal Sealift Agreement (VISA), and the Voluntary Tanker Agreement (VTA) administered by the Maritime Administration, DOD has maintained access to U.S. commercial capabilities and transportation networks while ensuring the continued viability of both the U.S.-flag fleet and the pool of citizen mariners who man those vessels.

What is your view of the importance of these Maritime Administration programs?

Answer. The MSP, VISA, and VTA are critical to TRANSCOM's ability to meet the needs of the warfighter and the Nation. For more than a decade of operations

in Iraq and Afghanistan, our commercial sealift partners have provided the vast majority of sealift for DOD. The vessel capacity, intermodal transportation networks and the U.S. Citizen Merchant Marine are key components to TRANSCOM and its global mission.

Question. What changes in these programs, if any, do you believe are appropriate and would make them more effective or more efficient in supporting DOD transportation requirements?

Answer. The ability of these programs to meet DOD needs is directly tied to the health of the U.S.-flag international fleet, which has been declining in size for some time. Additionally, as force drawdowns continue in Afghanistan, so will the deployment and sustainment cargoes which have become a valuable piece of our commercial partners' business. In recognition of these dynamics, Congress tasked the Maritime Administration with the development of a National Maritime Strategy to ensure the health of the fleet and the U.S. Merchant Marine. TRANSCOM is coordinating closely with MARAD to ensure these vital commercial programs remain effective in supporting DOD well into the future.

CIVIL RESERVE AIR FLEET

Question. The Air Force has in the past, and may very well in the future, rely heavily on the Civil Reserve Air Fleet (CRAF) to supplement its organic airlift. The National Defense Authorization Act (NDAA) for Fiscal Year 2014 requires the Secretary of Defense to provide an assessment of the requirement to maintain industrial base for CRAF carriers and ability of CRAF carriers to support the goals of the National Airlift Policy.

What is your assessment of CRAF's ability to meet requirements to transport any equipment, materials, or commodities for the use of U.S. military operations and respond to a humanitarian disaster?

Answer. We rely on our commercial partners as an integral part of providing global air lift assets to support military operations and in response to humanitarian disasters. In addition to our organic capability, commercial carriers that participate in CRAF provide the augmentation capability that allows us to say "Yes" to any call our Nation makes of us. The combined capability of military and commercial lift gives us the ability to transport equipment, materials, or commodities the warfighter will need to execute their mission to any point on the globe. To ensure the strength of our CRAF partnership and the program's continued viability, TRANSCOM conducts biannual Executive Working Group (EWG) conferences to bring together Chief Executive Officers, Presidents, and other representatives of the commercial airline industry to discuss vital issues affecting the program. The CRAF EWG will continue to meet on a regular basis to discuss future changes as we strive to maintain the readiness of the program to support our Nation. If confirmed, I will continue to work with our CRAF partners to ensure the business relationships remain solid and the contracts continue to support DOD requirements.

Question. Do the changes in the commercial airline industry, characterized by bankruptcies and a move toward smaller and shorter-range aircraft, impact the future viability of the CRAF system?

Answer. The commercial airline industry is dynamic and always has been. We have been able to adapt to carrier's fleet planning and benefited by having a commercial augmentation capability ready to answer the call when needed. It is accurate there are fewer carriers in the CRAF program now than 15+ years ago. I have, however, met with several airline executives over the past 18 months, and to the person, they have all said they will support the DOD and CRAF program because it is the right thing to do for our Nation. It is also accurate to say as we drawdown forces from Afghanistan, there will be excess capacity in the commercial sector that we expect to go away as carriers right size their fleets to meet the new business environment. Through AMC sponsored research, conducted as part of an extensive ongoing CRAF study, we are confident the CRAF program will remain viable and able to meet operational plans in the future.

Question. Do you think it is important to maintain an adequate industrial base for CRAF carriers?

Answer. CRAF has been a healthy program for over 60 years. It is a capability that no other nation can replicate and ensures we can meet national requirements that our organic assets alone cannot provide in times of crisis or conflict. It is critical we maintain both an organic airlift capability and commercial augmentation capability that is "ready" to answer the call when the next crisis arises. Striking a balance of airlift opportunities in this fiscally constrained environment is one of the biggest challenges we face going forward. If confirmed, I will work with all concerned to define a minimum business level for our commercial partners that will en-

sure we maintain readiness, not only for the carriers, but also for the Defense Transportation System.

Question. How much should we be relying on CRAF to meet our peacetime and wartime airlift requirements?

Answer. The CRAF program is a critical component in this nation's ability to rapidly deploy forces and equipment in times of crisis and peace. Because of the capability our commercial partners bring to the fight, we can deploy forces more rapidly and more efficiently than any other nation in the world. In peacetime, this workload changes from year-to-year due to dynamic customer requirements. Our forecast requirements are expected to be much lower starting in fiscal year 2016 compared to the past 13 years, which will impact both military and commercial capacity. We will continue to strive for the balance between military and commercial capacity.

Question. What changes, if any, do you think need to be made to CRAF—authorities, requirements, composition?

Answer. AMC, in coordination with TRANSCOM, chartered a study of the CRAF program to look at these specific issues. Throughout the study we engaged industry experts for their advice on where the airline industry is headed and what to expect. The study team provided recommendations to senior leadership and industry executives. We are in the process of analyzing carrier feedback and revising the appropriate recommendations for senior leaders' decision. The results of this study are expected to be complete no later than June of this year, and I have committed to report the results of that study to interested Members of Congress at that time.

QUADRENNIAL DEFENSE REVIEW

Question. What is your view of the QDR process? Was TRANSCOM asked to provide inputs to the QDR prior to it being finalized?

Answer. I view the QDR process as vital to the future success of DOD to prevail in current operations, deter our enemies, and ensure success in any future conflicts. It is essential for all the combatant commands and Services to meet, discuss strategic and current issues, and come to agreement on the direction ahead for DOD for defense of our Nation.

TRANSCOM was an active participant in the 2014 QDR process to include discussions on DOD strategy, implications of budget reductions, and Force Posture. In addition, TRANSCOM coordinated with Air Force leadership in the development of the tactical and strategic airlift requirements. As previously mentioned, the sealift requirements were not defined as main elements in the Navy fiscal year 2019 force structure.

READINESS

Question. Why did TRANSCOM recently downgrade its overall readiness assessment?

Answer. It's my understanding that TRANSCOM's overall readiness assessment has been the same for more than 3 years and the current overall assessment is consistent with that trend. While current readiness levels are assessed as sufficient for operations, projected readiness levels are of concern and must also take into account the long-term effects of sequestration and funding reductions. TRANSCOM's readiness is dependent upon the long-term health of strategic airlift, surge sealift and other enabling capabilities that face significant challenges in times of budget uncertainty. Modernization, recapitalization, and balanced use of both organic and commercial lift are necessary to maintain agreements and readiness levels across the transportation and logistics enterprise.

Also, because TRANSCOM must communicate over the unclassified networks with many private-sector entities in the transportation and shipping industry, protecting command and control systems from attack is a huge challenge to readiness. If I am confirmed, I will continue to advocate for improved security standards, incident reporting, and cyber defense capabilities across TRANSCOM's mission responsibilities.

TRANSCOM RISKS

Question. What is your assessment of TRANSCOM's critical risks and key issues based on sequestration budget funding level?

Answer. The reduced customer workload will drive impacts to organic and commercial capabilities that will likely be required in the future with potential readiness impacts on the organic and commercial transportation and logistics networks we rely on. Budgetary uncertainty makes it difficult to posture and plan for our customer's future transportation and logistics workload demand, as well as ensure all readiness and mobility capability aspects (people, infrastructure, assets) of our mission are preserved. The value of TRANSCOM being funded through a working cap-

ital fund (TWCF) is that the command can focus on long-term requirements and not make near-term suboptimal decisions.

CYBERSPACE OPERATIONS AND SECURITY

Question. Transportation Command must communicate over the unclassified Internet with many private-sector entities that are central to DOD's force generation and deployment operations—in the transportation and shipping industries in particular. Much of the rest of the critical communications and operations of the Defense Department can be conducted over the classified DOD internet service, which is not connected to the public Internet and is therefore much more protected against eavesdropping, espionage, and/or disruption by computer network attacks.

What do you believe are the critical needs of TRANSCOM for cyber security?

Answer. TRANSCOM moves vast amounts of information between military and commercial partners in its role as the distribution process owner for the Department. Command and control systems must get the right information to the right people at the right time, while protecting it from adversaries. If confirmed, I will continue the work to protect the command's information equities by working with our agency and commercial partners to further define roles, responsibilities, relationships and authorities for cyber security and to build trust and enhance information sharing.

Question. What plans do you have for addressing these critical needs?

Answer. TRANSCOM will need to continue addressing cyber issues on multiple fronts. Keeping command and control systems secure and protecting them from attack is a huge challenge. TRANSCOM has led the way in developing cyber language in its contracts to address security standards and incident reporting which, if confirmed, I will continue to push. In addition, I will continue the migration of component command and control systems inside the TRANSCOM security perimeter which will provide better situational awareness to my cyber security teams. I will also continue to collaborate with U.S. Cyber Command (CYBERCOM) and our Defense Information Systems Agency (DISA) partners to incorporate a solid command and control infrastructure that improves the accuracy and timeliness of cyber defense information providing synchronization of cyber operations across TRANSCOM's mission threats.

Question. How important is it that TRANSCOM be aware of cyber intrusions by advanced persistent threat (APT) actors into the networks of airlines, shippers, and other defense contractors that enable TRANSCOM operations?

Answer. Commercial partners provide volume, velocity and efficiency that make TRANSCOM's mission possible. Vulnerabilities within any organization's infrastructure, including cyber vulnerabilities, are a risk for all mission partners. TRANSCOM data that resides on our commercial partners' networks, if compromised by an APT, is a potential cyber security issue that, at minimum, provides insight into TRANSCOM operations. It is critical that we have awareness of these intrusions so that we can mitigate their operational impacts in the other domains.

Question. Are you concerned about the level of reporting of cyber events by command contractors or other U.S. Government agencies to TRANSCOM?

Answer. The level of reporting continues to be a concern. TRANSCOM has overcome some of these challenges with its cyber contract language and partnering efforts. The next step is to work with our commercial partners to develop a measurable standard of compliance.

Question. When TRANSCOM becomes aware of an APT intrusion into an operationally critical contractor, what steps should the command take to determine whether operational plans should be adjusted to mitigate the risk of the intrusion affecting military operations?

Answer. The level of reporting continues to be a concern. TRANSCOM has overcome some of these challenges with its cyber contract language and partnering efforts. If confirmed, I will work with all stakeholders, government, military, and commercial partners to define the steps necessary to adjust to cyber attacks, including APT intrusions.

Question. Is DOD taking adequate steps to address your special needs?

Answer. It is my understanding that TRANSCOM works very closely with DOD to share information on cyber security, intelligence and logistics operations to assess overall impact of cyber intrusions to the command's mission. Due to the high volume of the command's workload conducted on unclassified systems, the Department's use of cross-cutting teams including CYBERCOM, DISA, and various intelligence agencies is necessary to protect mission critical information.

RESEARCH AND DEVELOPMENT

Question. TRANSCOM's budget includes funding for a research and development activity designed to allow for examination and improvement of the entire supply chain as part of TRANSCOM's role as Distribution Process Owner.

What are the major gaps in capability related to TRANSCOM's mission that need to be addressed through research and development efforts?

Answer. Research and Development (R&D) investments will play an essential role in addressing a variety of challenges and capability gaps to ensure TRANSCOM's ability to accomplish its mission in an ever-increasing contested cyberspace and Anti-Access/Area Denial (A2/AD) environment. New technologies may allow TRANSCOM to improve the efficiency and effectiveness of distribution operations and lower the operating costs for our Nation's joint logistics enterprise. If confirmed, I will champion TRANSCOM's R&D investment priorities to address these challenges and capability gaps while improving our effectiveness and efficiency by exploring and further developing technologies in the areas of End-to-End Visibility, Command and Control/Optimization/Modeling and Simulation, Cyber, and Global Access.

Question. What unique processes and technologies do you feel TRANSCOM needs to develop through its own program and investments?

Answer. As the DOD's Distribution Process Owner and Global Distribution Synchronizer, TRANSCOM must continue the business process management work begun under the Agile Transportation for the 21st Century program. Distribution processes should be designed, documented and/or refined in three distinct areas (e.g. Requirements Management, Network Design, and Capacity Management). In addition, TRANSCOM continues to enhance warfighter support with a range of technologies with particular emphasis on addressing A2/AD challenges. If confirmed, I will pursue and support innovative solutions which improve efficiency, effectiveness, and maintain organic readiness to support the Nation's global missions.

Question. How will you work with other research and development organizations to ensure that TRANSCOM's current and future capability gaps are addressed?

Answer. TRANSCOM annually engages combatant commands, Services, Office of the Secretary of Defense, DLA, the Joint Staff, other Government agencies, and academia S&T communities for updates and validation of joint deployment and distribution technology gaps and focus areas which guides our Research, Development, Test, and Evaluation (RDT&E) investments. Nearly 75 percent of our RDT&E projects are collaboratively funded which greatly increases the transition of efficiency-gaining, life-saving, and cost-reducing capabilities to the warfighter. If confirmed, I will continue to partner with these organizations to identify, validate and recommend RDT&E projects that address validated capability gaps.

TECHNOLOGY PRIORITIES

Question. Serving the needs of the combatant commanders both in the near term and in the future is one of the key goals of the Department's science and technology (S&T) executives, who list outreach to commanders as an activity of continued focus.

What do you see as the most challenging technological needs or capability gaps facing TRANSCOM in its mission to provide air, land, and sea transportation to DOD?

Answer. Primary concern will be developing and exploiting emerging technologies that improve the Department's ability to provide timely and precise delivery of sustainment to our warfighters as well as humanitarian aid and relief anywhere, in moment's notice, and in a fiscally responsible manner. Additionally, we need to explore information security and assurance as well as new cyber technologies to ensure greater efficiency and mission accomplishment. Furthermore, reducing dependency on fossil fuels will also remain a major focus area for TRANSCOM.

Question. What would you do, if confirmed, to make your technology requirements known to the department's S&T community to ensure the availability of needed equipment and capabilities in the long term?

Answer. If confirmed, I will work through appropriate S&T community forums including Joint Interagency Field Experimentations, Defense Innovation Marketplace, technology symposiums, and collaborative interservice/agency partnerships to preserve our 90 percent transition rate of proven technologies.

TECHNOLOGY TRANSITION

Question. TRANSCOM has been active in the Joint Capability Technology Demonstration (JCTD) process.

What are your views on the JCTD process as a means to spiral emerging technologies into use to confront changing threats and to meet warfighter needs?

Answer. The Department's JCTD program is an extremely effective tool that combatant commands leverage to rapidly develop and insert emerging technologies to address warfighter needs and capability gaps. In contributing to TRANSCOM's successful JCTD track record, if confirmed, I will strongly advocate for innovative technologies which enhance warfighter support and success.

Question. What steps will you take, if confirmed, to enhance the effectiveness of technology transition efforts within your command and in cooperation with other Services and defense agencies?

Answer. If confirmed, I will continue to apply the Command's RDT&E investments, in partnership with other combatant commands, Services, Defense Agencies, academia, and industry to advance our Nation's war fighting capabilities. I will work with stakeholders in leveraging the Department's many programs (JCTD, Coalition Warfare Program, Joint Test & Evaluation, Small Business Innovative Research, etc.) to rapidly develop, field, and transition mature technologies that address near term needs and identified gaps. Specifically, I will partner with our stakeholders to vet projects, gain buy-in, and avoid duplication. Finally, I will ensure that all projects develop a viable transition strategy and emphasize rapid fielding from day one.

DEPLOYMENT CHALLENGES

Question. Multiple studies by TRANSCOM and the Army, and direct experience in Afghanistan and elsewhere, demonstrate that the airlift strategy and airlift platforms developed for the Cold War confrontation in Central Europe are not ideal to support operations in third-world regions. Unlike Europe, most of the world has few airfields with long runways, and there are fewer still that have parking space for more than a couple of cargo aircraft to unload at one time. This "Maximum-on-Ground" (MOG) metric is the critical measure of throughput capacity at airfields. The few airfields with MOG greater than 2 are scarce and are located within major urban areas, usually far from where ground forces would be employed. Traditional fixed-wing airlifters—even flexible ones like the C–17—cannot be effectively employed in large numbers to deploy and support ground forces in these regions because of these infrastructure limitations.

Previous analyses have indicated that alternatives to traditional fixed-wing transports, such as heavy-lift airships and heavy vertical take-off and landing (VTOL) rotorcraft, scored very high compare to current programs. These alternatives could deploy more forces faster, save lots of fuel, and increase sustainment. Because they deliver troops and supplies directly to the point of need, they could reduce the number of trucks on the road that are vulnerable to IEDs, as well as the length of supply lines. In other words, they would also reduce the vulnerability of our supply lines and save lives.

What is your view of these analyses?

Answer. My understanding is the Joint Future Theater Lift Technology Study (JFTL TS) was completed on 20 February 2013. The intent of the JFTL TS was to evaluate options to supplement the C–17, C–130, and C–27 capabilities to deliver medium weight combat vehicles into very austere environments. The JFTL TS assessed the overall value and cost of a variety of fixed wing aircraft, hybrid airships and tilt-rotor platforms as to how they might perform in emerging, future intra-theater airlift missions. The JFTL TS was comprehensive and provided insight to the cost effectiveness and risk of multiple technology options.

Question. We understand that the Army favors a heavy lift, second generation tilt rotor that would provide VTOL capabilities.

Answer. I understand that in the view of the JFTL TS, the Tilt Rotor (TR) technology alternative is the most operationally effective technology alternative because it is not restrained to fixed airfields; is capable of taking off and landing at more opportune landing sites (i.e., austere, short, unimproved landing areas), and is not limited by traditional Maximum on Ground (MOG) concepts. I believe it is reasonable to continue to examine these conclusions in the context of maturing CONOPs and anticipated schemes of maneuvers. It is also important to understand the maturity of the technologies that are necessary to develop heavy VTOL capabilities. If confirmed, I will assure that TRANSCOM will continue to monitor development of all emerging VTOL capabilities.

Question. Do you support development of such a platform?

Answer. Development of heavy lift Tilt Rotor or Hybrid Airship platforms will require careful consideration of our current and future warfighting needs, the planned fiscal environment, and our ability to mature both the technologies and operational

concepts to make these delivery options operationally viable. While these platforms may fill future capability gaps of emerging warfighting concepts, they both would require significant investment to develop and field. At this time, a hybrid airship configured for heavy cargo, equivalent to legacy lift platforms, does not exist. I believe the DOD should support technology development which may lead to a commercially produced hybrid airship capability in the future.

Question. In natural disasters, the airfields and roads and bridges that are required to fly in and distribute relief forces and supplies are frequently destroyed. Fixed-wing transports that need functioning airfields are not much use, but vertical lift aircraft or airships have the potential for continuing effective operations.

Do you believe that the TRANSCOM analyses have adequately factored disaster relief into their assessments?

Answer. Yes, the MCA included a number of disaster relief scenarios and found that "PB13 mobility forces do not materially constrain the U.S. objectives associated with conducting simultaneous operations in different theaters, and have sufficient capabilities to concurrently support a heightened defense posture in and around the United States or support U.S. civil authorities in response to a large-scale attack or natural disaster.

Question. How would you assess TRANSCOM's ability to respond to domestic disaster relief?

Answer. Based on the results of the MCA and TRANSCOM's ongoing planning with U.S. Northern Command, the Command, in partnership with the National Guard and local authorities, can effectively respond to and support domestic disaster relief efforts as needed.

DEFENSE PERSONAL PROPERTY SYSTEM

Question. For over 10 years, TRANSCOM and its subordinate command, Surface Deployment and Distribution Command, have been working to improve the process of moving servicemembers' household goods and gaining the support of the transportation provider industry for needed changes. Implementation of the new system—Defense Personal Property System (DPPS)—uses a "best value" approach to contracting with movers that focuses on quality of performance, web-based scheduling and tracking of shipments, servicemember involvement throughout the moving process, and a claims system that provides full replacement value for damaged household goods. Successful implementation of this system depends on replacement of the legacy Transportation Operational Personal Property Standard System (TOPS) with the web-based DPPS.

What do you view as the most significant challenges that remain in continuing to implement DPPS?

Answer. TRANSCOM is currently incorporating the remaining functionality for Non-Temporary Storage, Intra-Country Moves, and Direct Procurement Method into DPPS while modernizing the architecture to enhance overall system performance and the user experience. TRANSCOM recently re-competed a development and sustainment contract, which was awarded 9 Oct 2013. One of the most significant challenges that remain is ensuring capability development maintains schedule to enable the sunset of the legacy TOPS in fiscal year 2018.

Question. What is your assessment of the performance of DPPS in achieving the requirement for full replacement value for damaged or missing household goods claims?

Answer. Full replacement value is implemented across the Services for all modes of shipments in support of the Defense Personal Property Program. It is my understanding that the existing claims module is scheduled for redesign and will be deployed in fiscal year 2016 to improve the user experience. If confirmed, I will ensure improvements such as this continue.

Question. What is your understanding under DPPS of the percentage of valid personal claims for damage or loss of household goods that is currently paid for by DOD and the percentage that is paid for by the movers who caused the damage?

Answer. In 2013 less than 9 percent of submitted claims were transferred to the Military Claims Offices (MCOs). The MCOs are normally able to recover approximately 80–90 percent of what they pay out from the Transportation Service Provider (TSP). My understanding is TSPs settle most claims directly with the servicemember.

Question. What is your assessment of the adequacy of the response rate on customer satisfaction surveys as a method for identifying best and worst performers?

Answer. Customer Satisfaction Survey response rates have risen to 40 percent. With 553,000 personal property moves in 2013, the survey response rates continue to be statistically significant. Survey response rates are the cornerstone for ensuring

that quality transportation service providers are participating in the program, and opportunities for struggling performers are minimized or eliminated. If confirmed, I will continue to work closely with the Service Headquarters to increase the survey response rates.

Question. If confirmed, what role would you play in ensuring that DPPS is fully funded and implemented and will you make every effort to ensure this program is successful in meeting its goals?

Answer. If confirmed, I will leverage DPPS to continue to improve our business processes for household goods and services. OSD, Joint Staff, and the Services have committed to fully fund the DPPS program development and sustainment between fiscal year 2014–2018. I will work to ensure the DPPS program successfully meets the Services' goals to fully support servicemembers' personal property moves.

SPACE AVAILABLE TRAVEL POLICIES

Question. DOD, in consultation with TRANSCOM, submitted a report to Congress on Space Available Travel for Certain Disabled Veterans and Gray-Area Retirees in December 2007. The report concluded that increases in space available eligibility would significantly impact DOD's ability to accomplish effectively the airlift mission and negatively affect support to active duty military space available travelers. Additionally, the report concluded that adding to the eligibility pool would increase support costs and displace the current policy that mandates that space-available travel not incur additional costs to dod.

Do you consider the conclusions and recommendations of the December 2007 report to still be valid?

Answer. I believe the conclusions and recommendations of the December 2007 report remain valid. Also, I believe DOD's concern with any expansion to the Space-Available program was also reiterated in the GAO review as directed by section 362 of the NDAA for Fiscal Year 2012. DOD data showed the five most used air terminals had limited seats available with the three most traveled destinations from each terminal were near capacity. An expansion to the current pool of eligible travelers limits the ability to support the primary objective of the space available program which is to enhance the morale and welfare of our Active-Duty Force.

Question. What are the constraints in today's operational environment of expanding the categories of individuals eligible for space available travel?

Answer. I believe the conclusions and recommendations of the December 2007 report remain valid. Also, I believe DOD's concern with any expansion to the space available program was also reiterated in the GAO review as directed by section 362 of the NDAA for Fiscal Year 2012. We will work closely with DOD as the Secretary of Defense reviews space available policy in accordance with the NDAA for Fiscal Year 2013.

Question. What recommendations, if any, do you have regarding changes to the existing policies controlling space available travel eligibility?

Answer. In today's operational environment, DOD has limited ability to support continued expansion of the space available program. We will work closely with DOD as the Secretary of Defense reviews space available policy in accordance with the NDAA for Fiscal Year 2013.

CONGRESSIONAL OVERSIGHT

Question. In order to exercise its legislative and oversight responsibilities, it is important that this committee and other appropriate committees of Congress are able to receive testimony, briefings, and other communications of information.

Do you agree, if confirmed for this high position, to appear before this committee and other appropriate committees of Congress?

Answer. Yes.

Question. Do you agree, when asked, to give your personal views, even if those views differ from the administration in power?

Answer. Yes.

Question. Do you agree, if confirmed, to appear before this committee, or designated members of this committee, and provide information, subject to appropriate and necessary security protection, with respect to your responsibilities as the Commander, TRANSCOM?

Answer. Yes.

Question. Do you agree to ensure that testimony, briefings, and other communications of information are provided to this committee and its staff and other appropriate committees?

Answer. Yes.

Question. Do you agree to provide documents, including copies of electronic forms of communication, in a timely manner when requested by a duly constituted committee, or to consult with the committee regarding the basis for any good faith delay or denial in providing such documents?

Answer. Yes.

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR BILL NELSON

CIVIL RESERVE AIR FLEET

1. Senator NELSON. General Selva, in your response to the advance policy questions, you stated, "In peacetime, the [airlift] workload changes from year-to-year due to dynamic customer requirements. Our forecast requirements are expected to be much lower starting in fiscal year 2016 compared to the past 13 years, which will impact both military and commercial capacity." Based on the lowered requirement for airlift, can the Transportation Working Capital Fund accounts adequately support both crew readiness requirements and the Civil Reserve Air Fleet (CRAF) program?

General SELVA. Over the last 13 years of supporting Overseas Contingency Operation requirements U.S. Transportation Command (TRANSCOM) has been able to maintain organic crew readiness while also supporting the CRAF. However, the current and future workload projections are significantly decreased due to the Afghanistan drawdown and Services' constrained transportation budgets. When TRANSCOM reaches a point where it can no longer reduce capacity supplied to match lower workload due to Service readiness requirements, the Transportation Working Capital Fund will realize a loss and our component command readiness will be impacted as no revenue is generated. Working Capital Fund policy dictates these losses become the responsibility of the Services and/or recouped by increased future rates.

We have efforts underway regarding the CRAF to support the lower business levels. First, we have provided CRAF subscribers with business projections, which will help them size their fleets to meet their own requirements. Second, we are working to establish a minimum level of business to support commercial readiness and business. This will help support not only the CRAF subscribers, but also our military aerial ports to ensure they maintain readiness and familiarization with utilizing commercial aircraft.

2. Senator NELSON. General Selva, are the training needs of our current airlift fleet negatively affecting CRAF carriers?

General SELVA. Ensuring the readiness of the CRAF while maintaining an organic fleet capable of meeting all DOD requirements is a priority for us and it requires the right balance of workload between the military and commercial segments. Achieving that balance for the future requires a careful analysis of commercial and military readiness requirements, capabilities required for all levels of response, and an understanding of economic factors affecting the industry's ability to meet DOD requirements. We are working through that analysis now.

Recognizing the need to maintain a viable CRAF and the likelihood of both declining budgets and workload post-Afghanistan, our comprehensive review of the CRAF program is focused on the objective of developing recommended changes to assure the program's viability in the future and the readiness of participating carriers. We recognize the need for CRAF carriers to have business within the defense transportation system to maintain their readiness to support DOD.

We also need to continue to season Active Duty and Air Reserve component airman and maintain a ready organic airlift capability. Air Mobility Command is working to balance this requirement, as well as certain combatant commander requirements that dictate use of organic assets with the need to maintain a ready commercial augmentation capability.

3. Senator NELSON. General Selva, what are your plans to ensure the future viability of the CRAF program?

General SELVA. In the midst of declining business, TRANSCOM has made significant efforts to bolster relations with the commercial airline industry through military and industry joint venues. The CRAF Executive Working Group, National Defense Transportation Association, and the Military Aviation Advisory Committee are

examples of venues which work to develop solutions and exchange ideas to effectively ensure the future viability of the CRAF program.

We have listened to industry concerns and have pursued multiple avenues to maximize business opportunities, not only by pursuing CRAF preferences in policy, but adjusting operating procedures and guidance to maximize workload to our U.S. flag carriers. Additionally, we have been proactive and transparent in giving our industry partners the most accurate projected requirements during this drawdown period so commercial carriers can posture themselves appropriately. In addition to these efforts, we conducted a comprehensive review of the CRAF program with an objective of developing recommended changes to assure the program's viability in the future.

QUESTIONS SUBMITTED BY SENATOR JOE MANCHIN III

EQUIPMENT LEFT BEHIND IN IRAQ AND AFGHANISTAN

4. Senator MANCHIN. General Selva, I am very concerned about the amount of equipment that the United States will be forced to leave in Afghanistan. I understand that the United States will not be able to recover a substantial amount of military equipment from Afghanistan. What is your assessment of the amount of equipment the United States will be forced to leave in Afghanistan?

General SELVA. The Services have made decisions on some of their equipment that will be returning to the United States and TRANSCOM will transport it when and where needed. The Services are still deciding on disposition of equipment that may be destroyed in place or declared excess and offered to other countries as Excess Defense Articles.

5. Senator MANCHIN. General Selva, what is the value of this equipment and what will be the associated costs with removing and destroying the sensitive components among this arsenal?

General SELVA. The Services are in the best position to provide an overall cost analysis of equipment in theater. TRANSCOM assists the Services with calculating the transportation cost and readily supports equipment movement once the Services determine what is to be moved out of theater.

6. Senator MANCHIN. General Selva, is there an existing plan to recoup these losses, perhaps through Foreign Military Sales (FMS)?

General SELVA. The Services are in the best position to provide an answer on their equipment replacement plans. Defense Security Cooperation Agency is in the best position to provide an answer on any possible recoupment of funds through FMS sales to offset equipment losses.

7. Senator MANCHIN. General Selva, does this compare to the amount and value of equipment that the United States failed to retrograde from Iraq?

General SELVA. The Services are in the best position to provide an answer on the amount of equipment that was not retrograded from Iraq. TRANSCOM assisted in transporting equipment from Iraq once disposition decisions were made.

QUESTIONS SUBMITTED BY SENATOR KIRSTEN E. GILLIBRAND

CYBER ATTACKS ON U.S. TRANSPORTATION COMMAND

8. Senator GILLIBRAND. General Selva, this committee is currently reviewing a report on cyber attacks on TRANSCOM dating from fiscal year 2011. I am highly concerned about this information in light of the fact that TRANSCOM will be instrumental as we leave Afghanistan. If confirmed, how do you intend to handle this issue?

General SELVA. We have migrated the critical Transportation Component Command systems behind the TRANSCOM security boundary and exercise command and control over the defenses of those systems. These efforts align with the Department's Joint Information Environment initiative, as we are implementing a security architecture that fits within DOD's security architecture, led by the DOD CIO and the Defense Information System Agency (DISA). We expect to achieve significant efficiencies by leveraging common enterprise services and improving our cyber security posture.

9. Senator GILLIBRAND. General Selva, from your perspective, what can we do to improve cyber defenses as they relate to contractors?

General SELVA. TRANSCOM actively engages with our commercial partners on cyber security; we have led multiple commercial partner outreach programs and highly encourage them to join the Defense Industrial Base Cyber Security/Info Assurance program. Of the 80 current TRANSCOM commercial partners that we encouraged to participate in the Defense Industrial Base Cyber Security/Information Assurance Program, only 7 are full participants. Three additional companies have requested further information and are considering joining. In addition we have developed cyber security contract language for both our commercial carriers and information technology (IT) support contracts that require notification in the event of an actual intrusion that impacts TRANSCOM mission data. In these cases we work with our commercial partners and through law enforcement and contracting channels to mitigate the threat to mission and improve cyber defenses. We have recently streamlined some of that language changing reporting requirements from reporting intrusions affecting DOD data to reporting intrusions on any systems in which DOD data resides or transits. We also welcome the opportunity to help validate security controls with our commercial partners through voluntary exercises that will strengthen dialogue and a shared understanding of the threat to the TRANSCOM mission.

QUESTIONS SUBMITTED BY SENATOR JAMES M. INHOFE

NETWORK VULNERABILITY

10. Senator INHOFE. General Selva, TRANSCOM has been subject to a growing number of cyber attacks. TRANSCOM's reliance on unique contracts—such as the CRAF program where U.S. civil air carriers agree to augment organic military airlift during a crisis in exchange for access to peacetime defense business—creates unique challenges. In a contingency, TRANSCOM's ability to move troops or supplies could be hindered if a vendor's network were compromised. Today there appears to be little sharing of threat and network vulnerability information. Do you share these concerns?

General SELVA. TRANSCOM has always shared this concern which is why we work to make substantial progress in organizing and resourcing our TRANSCOM cyber defense efforts. We stood up our Joint Cyber Center on our Fusion Center operations floor to ensure our cyber defense efforts are aligned with our transportation mission. CYBERCOM has provided a Cyber Support Element that gives us reach back into their capabilities, and Air Force Cyber Command has provided a Cyber Protection Team that has just reached Initial Operational Capability, with another on the way. In addition to these DOD cyber defense capabilities, our Joint Cyber Center has established relationships with law enforcement and other federal and state agencies to buttress our cyberspace defenses. There are opportunities for improvement of information sharing between the special investigations units within the Department and their counterparts within the Department of Justice. Both can benefit from understanding the TRANSCOM mission context and our current vendor list so they can address TRANSCOM national security equities in the course of their ongoing operations.

11. Senator INHOFE. General Selva, what other unique cybersecurity challenges do you believe we should be aware of?

General SELVA. The primary challenge continues to be protection of mission data residing in or transiting the information systems of our commercial partners, which lie outside of DOD and TRANSCOM visibility, control, or authorities. Historically, TRANSCOM has encountered threat actors penetrating our military and commercial partner networks to gain access to our mission data which could disclose DOD operations, disrupt command and control of logistics movements, and have the potential to deny or degrade operations. The fact that we do utilize commercial partners across the enterprise means that some of our data resides on information systems that exist in the commercial business community. These systems provide volume, velocity, and efficiency for our TRANSCOM mission. To mitigate vulnerabilities, we are actively engaged with our commercial partners on cyber security both in our contracts and in our relationships with these companies. We also work with our interagency partners to provide context to the execution of their authorities and ongoing activities because cyber defense is a team effort where one organization's vulnerabilities are potential vulnerabilities for all.

12. Senator INHOFE. General Selva, what steps are TRANSCOM and CYBERCOM taking to address these vulnerabilities?

General SELVA. TRANSCOM is integrating critical systems operated by our service components behind a common security boundary with common technology and policies and enhanced situational awareness for TRANSCOM and component network defenders. In addition, TRANSCOM is including the new Defense Federal Acquisition Regulation Clause, "Safeguarding of Unclassified Controlled Technical Information" in all of our new non-transportation contracts, while retaining the Cyber Security language we previously developed in our transportation contracts. We are continuing to build relationships with our commercial partners and law enforcement to increase collaboration and incorporate contract language based on industry best practices. Additionally, I am gaining operational control of cyber protection teams to augment our organic network defense forces. This will enable a better protective posture across the TRANSCOM enterprise. We are fully engaged with CYBERCOM and Defense Information Systems Agency to work through command and control of these assigned forces. The command is satisfied with our efforts to date and will continue to leverage opportunities to improve as they present themselves.

13. Senator INHOFE. General Selva, can TRANSCOM and DOD enact a policy change that can make the fixes that you envision?

General SELVA. DOD is working with its U.S. Government counterparts to enact policy and process changes that will enable coordinated employment of existing law enforcement and military authorities and capabilities, as appropriate. TRANSCOM continues to focus on improving information sharing between our network defenders and our commercial partners in the private sector to the greatest extent feasible in the current environment.

14. Senator INHOFE. General Selva, do you feel that TRANSCOM and DOD need more legislative authority to fix this persistent threat brought about by the current cyber intrusion problem?

General SELVA. The President has the necessary authority to order military action to defend our nation against all attacks including those in the cyber domain. The President can delegate authorities to the Secretary of Defense in order to use the Department's operational capabilities to defend against such an attack so additional legislative authority for DOD is not necessary. However, TRANSCOM and its industry partners serve to highlight that with so much of the critical infrastructure owned and operated by private industry, the government has limited visibility and thus is often unaware of the malicious activity targeting our critical infrastructure. These blind spots prevent the Government from being positioned to either help the critical infrastructure to defend itself or to defend the nation from an attack. The contract language in place at TRANSCOM, relationships we are building to enhance mission context with other agencies, and aligning our cyber defense resources are the ways in which we are addressing this issue.

QUESTIONS SUBMITTED BY SENATOR JOHN MCCAIN

AFGHANISTAN EQUIPMENT RETROGRADE

15. Senator MCCAIN. General Selva, in your testimony, you agreed that TRANSCOM was "on track to remove all the necessary equipment and armaments from Afghanistan by the end of 2014." How much U.S. military equipment do you assume will be left in Afghanistan? Please provide your answer as a percentage of total equipment currently in theater, as a dollar amount, or by some other meaningfully quantitative measure.

General SELVA. TRANSCOM provides common-user strategic lift on a global basis to our supported geographic combatant commands (GCCs). While we determine strategic sea, air, and surface lift feasibility to meet the transportation needs of the GCCs, we are not involved in determining equipment levels they require to execute missions in their Areas of Operation. In the case of Operation Enduring Freedom drawdown and the post-2014 enduring mission in Afghanistan, U.S. Central Command (CENTCOM), in coordination with the Military Services, will determine how much U.S. military equipment will be required to execute their assigned missions. As a supporting command in this effort, TRANSCOM is postured to generate the required strategic lift capacity to meet the Commander International Security Assistance Force drawdown timelines, and will continue to rely on our ground forces to identify and generate cargo for strategic lift to meet CENTCOM requirements. National level decisions associated with an approved and signed Bi-lateral Security

Agreement will heavily influence the final mission set required for CENTCOM operations in Afghanistan.

16. Senator MCCAIN. General Selva, to the best of your knowledge, what will be the disposition of any equipment left in Afghanistan after the departure of U.S. forces?

General SELVA. CENTCOM, in coordination with the Military Services, will determine the disposition of U.S. military equipment in Afghanistan after the departure of U.S. forces. Final disposition of this equipment will be influenced by national level decisions associated with an approved and signed Bilateral Security Agreement, which will significantly impact the equipment-set required to execute any enduring U.S. and coalition mission in Afghanistan. CENTCOM will determine final disposition based on operational requirements and transportation cost-benefit analysis in coordination with Office of the Secretary of Defense and Joint Staff. If strategic transportation is required, TRANSCOM is postured to fully support retrograde/redeployment of U.S. military equipment from Afghanistan, as well as Foreign Military Sales movements and Excess Defense Articles transfers when authorized and approved at appropriate DOD and congressional levels.

17. Senator MCCAIN. General Selva, please list the commands or agencies that provide guidance to TRANSCOM regarding retrograde of military equipment. In other words, do the combatant commander, the component commanders, the Services, or some combination of these have authority to decide what equipment is retrograded from Afghanistan?

General SELVA. TRANSCOM provides common-user strategic lift on a global basis to our supported geographic combatant commands (GCCs), based on transportation requirements that have been validated for movement by the GCC-in this case CENTCOM. While TRANSCOM determines strategic sea, air, and surface lift feasibility to meet the transportation needs of CENTCOM, we are not involved in determining which equipment will or will not be retrograded from Afghanistan. CENTCOM, in coordination with the Military Services, Office of the Secretary of Defense, and Joint Staff, will determine which U.S. military equipment will remain in Afghanistan for any enduring mission post-2014. As the strategic transportation provider, TRANSCOM is postured to generate the required strategic lift capacity to meet the Commander International Security Assistance Force drawdown timelines. We also continually present transportation feasibility and costing data to all stakeholders for their consideration when making final decisions on retrograde equipment disposition and transportation.

18. Senator MCCAIN. General Selva, you noted in testimony that five routes are used to get equipment and personnel in and out of country and that you are developing courses of action to bypass Russia. What is the status of the alternative logistics plan?

General SELVA. TRANSCOM has a flexible strategic network consisting of various lines of communication both in and out of Afghanistan. With multiple air and surface routes available, bypassing Russia for transit will have no significant impact on overall theater operations. If access to Russian air or surface routes becomes unavailable, we will route cargo to an alternate route with little to no affect on inbound or outbound flow.

19. Senator MCCAIN. General Selva, what assumptions with regard to the so-called southern route through Pakistan and northern routes through Russia are included in your assessment that TRANSCOM will have all necessary equipment out of Afghanistan by the end of 2014?

General SELVA. Currently, TRANSCOM moves less than 10 percent of retrograde cargo from Afghanistan via the Northern Distribution Network (NDN) through Russia, all of which can be diverted to other routes if required.

The Pakistan ground lines of communication (PAKGLOC) has achieved great velocity, but has also experienced challenges resulting in limited cargo flow in the past. Although the PAKGLOC is the preferred method of moving retrograde due to speed and cost, TRANSCOM is prepared to shift cargo to multi-modal and air direct operations as required. Albeit challenging with reduced ground line of communication access, TRANSCOM has the capacity to retrograde all necessary equipment from Afghanistan utilizing alternate transportation modes and routes provided the cargo is properly identified for strategic lift and prepared for movement in a timely manner.

20. Senator MCCAIN. General Selva, what would the impact be on TRANSCOM's equipment retrograde estimates if the northern ground road and rail routes were closed?

General SELVA. TRANSCOM supports warfighter and service priorities by providing a scalable transportation network that maximizes strategic flexibility and reduces operational risk across a variety of routes and modes, both into and out of Afghanistan. We continue to execute a variety of movement options utilizing both air and ground routes across the Northern Distribution Network, but historically these routes have accounted for a very low percentage of overall cargo. Loss of any strategic option increases risk, but ultimately TRANSCOM would be minimally affected by closure of the northern ground road and rail routes.

21. Senator MCCAIN. General Selva, what would the impact be on TRANSCOM's equipment retrograde estimates if the southern route was closed?

General SELVA. TRANSCOM works with its strategic partners to maintain an effective and flexible transportation network that includes air, ground and multimodal routes with organic and commercial capabilities. This robust structure minimizes reliance on any one nation, values fair and open competition, is reconfigurable and scalable, facilitating economic development and diplomatic engagement. The southern surface route (the Pakistan ground lines of communication) provides a low cost, potentially high volume option for retrograde operations, but ongoing issues (e.g. religious holidays, floods, political strife, and security concerns) have historically affected the volume of cargo and velocity of the route. TRANSCOM has successfully routed retrograde and redeploy cargo away from the PAKGLOC in the past with little to no affect on the strategic transportation network.

22. Senator MCCAIN. General Selva, you indicated during testimony that a business case would be applied to determine whether or not military equipment should be retrograded, disposed of via FMS, or given to allied or partner nations as grants. Do you have an accurate accounting of all U.S. military equipment in Afghanistan?

General SELVA. The Services are in the best position to provide an answer on their remaining equipment levels in Afghanistan. TRANSCOM will assist in transporting that equipment once disposition decisions are made.

23. Senator MCCAIN. General Selva, who makes the final disposition decision to lift, sell, or grant?

General SELVA. The Services are responsible for disposition decisions for their equipment. TRANSCOM then transports the equipment as needed. If U.S. defense articles are declared excess they can be made available for sale through the Foreign Military Sales program under the statutes of section 21 of the Arms Export Control Act or for grant transfer to eligible countries under the provisions of section 516 of the Foreign Assistance Act. The ultimate responsibility for determining if an item should be identified as excess rests with the Service having cognizance over the item.

When a country submits a request (via grant or sale) for excess defense articles (EDA), the Service evaluates and endorses the country request and submits it for review and staffing via Defense Security Cooperation Agency (DSCA) through the State Department, Commerce Department, and Office of the Secretary of Defense-Policy regional offices. If approved, DSCA prepares any required Congressional Notification. At the end of Congressional Notification, DSCA authorizes the Service to offer/transfer the EDA. Each fiscal year, the State Department Bureau of Political-Military Affairs, Office of Regional Security and Arms Transfers in coordination with DSCA identifies the countries eligible for grant EDA to Congress.

QUESTIONS SUBMITTED BY SENATOR KELLY AYOTTE

STRATEGIC AIRLIFT AIRCRAFT

24. Senator AYOTTE. General Selva, in your responses to the advance policy questions, you state that you support the plan to reduce the number of strategic airlift aircraft to a level of 275 aircraft. Yet, you acknowledge that certain scenarios presented some mobility challenges. Please describe what kind of scenario would present a challenge if our strategic airlift fleet drops to that level.

General SELVA. A force of 275 strategic airlift aircraft will support the national military strategy with acceptable risk. A force of 275 aircraft will be challenged to support the strategy in a situation where we are unable to produce sufficient functional aircraft operated by fully qualified crews. This could happen if crews have in-

sufficient flying hours to maintain qualifications or the aircraft are not maintained at adequate readiness levels.

25. Senator AYOTTE. General Selva, in your responses, you state that the Quadrennial Defense Review (QDR) recommended a force structure for the Air Force in fiscal year 2019 of 211 strategic airlift aircraft, 39 C–5s and 172 C–17s. If 275 strategic airlift aircraft presents challenges to TRANSCOM, what kind of challenges would 211 present?

General SELVA. The force of 39 C-5s and 172 C-17s referenced in the QDR 2014 reflect U.S. Air Force "combat coded" inventory; that is aircraft assigned to units for the performance of their wartime missions. That force becomes 275 total aircraft inventory (TAI) if backup aircraft inventory (BAI) and primary training aircraft inventory (PTAI) are included.

26. Senator AYOTTE. General Selva, would 211 strategic airlift aircraft be sufficient to support one and a half major combat operations?

General SELVA. The force of 211 strategic airlift aircraft (39 C–5s and 172 C–17s) referenced in the QDR 2014 reflects U.S. Air Force "combat coded" inventory; that is aircraft assigned to units for the performance of their wartime missions. That force of 211 "combat coded" inventory becomes 275 TAI if BAI and PTAI are included. A force of 275 strategic airlift aircraft will support the national military strategy with moderate risk.

27. Senator AYOTTE. General Selva, if our number of strategic airlift aircraft declines to 211, and a major combat operation were to begin, what kinds of delays might we confront in deploying Army ground units to a contingency in Korea, for example?

General SELVA. Based on TRANSCOM's analysis, we would expect any delays to be minor, but acceptable. Although the number of "combat coded" aircraft will decrease to 211 (with 24 additional aircraft assigned to BAI), the total size of the strategic airlift fleet remains at 275 (223 C–17s and 52 C 5Ms) TAI. During major combat operations, these additional 24 BAI aircraft are still available for contingency missions, but once added back to the fleet, would operate at a lower crew ratio, inducing manageable risk to force closure during sustained combat operations.

28. Senator AYOTTE. General Selva, would the delay in airlift be longer than is required to activate and train National Guard units?

General SELVA. No, the bulk of Army units moved at the onset of major crises are from the Active Component. However, those early deploying Army Reserve component units (U.S. Army Reserve and National Guard), as with the other Services' Reserve component units, are currently programmed to be ready to meet their planned early availability dates. Reserve component units requiring formal training or more lengthy activation processes prior to deploying are not generally associated with this early deployment period.

[The nomination reference of Gen. Paul J. Selva, USAF, follows:]

NOMINATION REFERENCE AND REPORT

AS IN EXECUTIVE SESSION,
SENATE OF THE UNITED STATES,
February 6, 2014.

Ordered, That the following nomination be referred to the Committee on Armed Services:

The following named officer for appointment in the U.S. Air Force to the grade indicated while assigned to a position of importance and responsibility under title 10, U.S.C., section 601:

To be General.

Gen. Paul J. Selva, USAF, 5397.

[The biographical sketch of Gen. Paul J. Selva, USAF, which was transmitted to the committee at the time the nomination was referred, follows:]

BIOGRAPHICAL SKETCH OF GEN. PAUL J. SELVA, USAF

General Paul J. Selva is Commander, Air Mobility Command (AMC), Scott Air Force Base, IL. Air Mobility Command's mission is to provide rapid, global mobility and sustainment for America's Armed Forces. The command also plays a crucial role in providing humanitarian support at home and around the world. The men and women of AMC—Active Duty, Air National Guard, Air Force Reserve, and civilians—provide airlift, aerial refueling, special air mission and aeromedical evacuation.

General Selva graduated from the U.S. Air Force Academy in 1980, and completed undergraduate pilot training at Reese Air Force Base, TX. He has held numerous staff positions and has commanded at the squadron, group, wing and headquarters levels. Prior to his current assignment General Selva was the Vice Commander, Pacific Air Forces, Joint Base Pearl Harbor-Hickam, HI.

General Selva is a command pilot with more than 3,100 hours in the C–5, C–17A, C–141B, KC–10, KC–135A, and T–37.

Education:

1980 - Bachelor of Science degree in aeronautical engineering, U.S. Air Force Academy, Colorado Springs, CO.

1983 - Squadron Officer School, Maxwell Air Force Base (AFB), AL.

1984 - Master of Science degree in management and human relations, Abilene Christian University, Abilene, TX.

1992 - Distinguished graduate, Air Command and Staff College, Maxwell AFB, AL.

1992 - Master of Science degree in political science, Auburn University, Montgomery, AL.

1996 - National Defense Fellow, Secretary of Defense Strategic Studies Group, Rosslyn, VA.

Assignments:

From	To	Assignment
June 1980	July 1981	Student, undergraduate pilot training, Reese AFB, TX.
July 1981	December 1984	Co-pilot and aircraft commander, 917th Air Refueling Squadron, Dyess AFB, TX.
January 1984	December 1988	Co-pilot, aircraft commander, instructor pilot, and flight commander, 32nd Air Refueling Squadron, Barksdale AFB, LA.
January 1989	July 1991	Company grade adviser to Commander, Strategic Air Command, later, manager of offensive aircraft systems and executive officer, Deputy Chief of Staff, Plans and Resources, Headquarters Strategic Air Command, Offutt AFB, NE.
August 1991	July 1992	Student, Air Command and Staff College, Maxwell AFB, AL.
July 1992	June 1994	Instructor pilot and flight commander, 9th Air Refueling Squadron, later, Commander, 722nd Operations Support Squadron, March AFB, CA.
June 1994	June 1995	Commander, 9th Air Refueling Squadron, later, Deputy Commander, 60th Operations Group, Travis AFB, CA.
July 1995	June 1996	National Defense Fellow, Secretary of Defense Strategic Studies Group, Rosslyn, VA.
July 1996	August 1998	Assistant to the Director, Office of the Secretary of Defense for Net Assessment, the Pentagon, Washington, DC.
August 1998	July 2000	Commander, 60th Operations Group, Travis AFB, CA.
July 2000	June 2002	Commander, 62nd Airlift Wing, McChord AFB, WA.
June 2002	June 2003	Vice Commander, Tanker Airlift Control Center, Scott AFB, IL.
June 2003	November 2004	Commander, Tanker Airlift Control Center, Scott AFB, IL.
December 2004	August 2006	Director of Operations, U.S. Transportation Command, Scott AFB, IL.
August 2006	June 2007	Director, Air Force Strategic Planning, Deputy Chief of Staff for Strategic Plans and Programs, Headquarters U.S. Air Force, Washington, DC.
June 2007	October 2008	Director, Air Force Strategic Planning, Deputy Chief of Staff for Strategic Plans and Programs, Headquarters U.S. Air Force, and Director, Air Force QDR, Office of the Vice Chief of Staff, Washington, DC.
October 2008	October 2011	Assistant to the Chairman of the Joint Chiefs of Staff, Washington, DC.
October 2011	November 2012	Vice Commander, Pacific Air Forces, Joint-Base Pearl Harbor-Hickam, HI.
November 2012	Present	Commander, Air Mobility Command, Scott AFB, IL.

Summary of joint assignments:

From	To	Assignment
September 1996	August 1998	Assistant to the Director, Office of the Secretary of Defense for Net Assessment, the Pentagon, Washington, DC, as a lieutenant colonel.

From	To	Assignment
November 2004 ...	July 2006	Director of Operations and Logistics, U.S. Transportation Command, Scott AFB, IL, as a brigadier general.
October 2008	October 2011	Assistant to the Chairman of the Joint Chiefs of Staff, Washington, DC, as a lieutenant general.

Flight information:
Rating: Command pilot
Hours flown: More than 3,100
Aircraft flown: C–5, C–17A, C–141B, KC–10, KC–135A, and T–37

Major awards and decorations:
Defense Distinguished Service Medal
Distinguished Service Medal
Defense Superior Service Medal
Legion of Merit with two oak leaf clusters
Defense Meritorious Service Medal
Meritorious Service Medal with three oak leaf clusters
Air Force Commendation Medal
Air Force Achievement Medal
Joint Meritorious Unit Award
Combat Readiness Medal with two oak leaf clusters
National Defense Service Medal with bronze star
Armed Forces Expeditionary Medal with two bronze stars
Southwest Asia Service Medal with bronze star
Global War on Terrorism Service Medal
Armed Forces Service Medal

Effective dates of promotion:
Second Lieutenant, May 28, 1980
First Lieutenant, May 28, 1982
Captain, May 28, 1984
Major, January 1, 1990
Lieutenant Colonel, March 1, 1994
Colonel, September 1, 1998
Brigadier General, January 1, 2004
Major General, June 2, 2007
Lieutenant General, October 8, 2008
General, November 29, 2012

[The Committee on Armed Services requires certain senior military officers nominated by the President to positions requiring the advice and consent of the Senate to complete a form that details the biographical, financial, and other information of the nominee. The form executed by Gen. Paul J. Selva, USAF, in connection with his nomination follows:]

UNITED STATES SENATE

COMMITTEE ON ARMED SERVICES

Room SR–228

Washington, DC 20510–6050

(202) 224–3871

COMMITTEE ON ARMED SERVICES FORM

BIOGRAPHICAL AND FINANCIAL INFORMATION REQUESTED OF NOMINEES

INSTRUCTIONS TO THE NOMINEE: Complete all requested information. If more space is needed use an additional sheet and cite the part of the form and the question number (i.e. A–9, B–4) to which the continuation of your answer applies.

PART A—BIOGRAPHICAL INFORMATION

INSTRUCTIONS TO THE NOMINEE: Biographical information furnished in this part of the form will be made available in committee offices for public inspection prior to the hearings and will also be published in any hearing record as well as made available to the public.

1. **Name:** (Include any former names used.)
Paul J. Selva.

2. **Position to which nominated:**
Commander, U.S. Transportation Command.

3. **Date of nomination:**
February 6, 2014.

4. **Address:** (List current place of residence and office addresses.)
[Nominee responded and the information is contained in the committee's executive files.]

5. **Date and place of birth:**
September 27, 1958; Biloxi, MS

6. **Marital Status:** (Include maiden name of wife or husband's name.)
Married to Ricki S. Selva (Maiden Name: Smith).

7. **Names and ages of children:**
None.

8 **Government experience:** List any advisory, consultative, honorary or other part-time service or positions with Federal, State, or local governments, other than those listed in the service record extract provided to the committee by the executive branch.
None.

9. **Business relationships:** List all positions currently held as an officer, director, trustee, partner, proprietor, agent, representative, or consultant of any corporation, firm, partnership, or other business enterprise, educational, or other institution.
None.

10. **Memberships:** List all memberships and offices currently held in professional, fraternal, scholarly, civic, business, charitable, and other organizations.
Air Force Association - Member.
Airlift Tanker Association - Member.

11. **Honors and awards:** List all scholarships, fellowships, honorary society memberships, and any other special recognitions for outstanding service or achievements other than those listed on the service record extract provided to the committee by the executive branch.
None.

12. **Commitment to testify before Senate committees:** Do you agree, if confirmed, to appear and testify upon request before any duly constituted committee of the Senate?
Yes.

13. **Personal views:** Do you agree, when asked before any duly constituted committee of Congress, to give your personal views, even if those views differ from the administration in power?
Yes.

[The nominee responded to the questions in Parts B–E of the committee questionnaire. The text of the questionnaire is set forth in the Appendix to this volume. The nominee's answers to Parts B–E are contained in the committee's executive files.]

SIGNATURE AND DATE

I hereby state that I have read and signed the foregoing Statement on Biographical and Financial Information and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

PAUL J. SELVA, GENERAL, USAF.

This 5th day of November, 2014.

[The nomination of Gen. Paul J. Selva, USAF, was reported to the Senate by Chairman Levin on March 26, 2014, with the recommendation that the nomination be confirmed. The nomination was confirmed by the Senate on April 8, 2014.]

[Prepared questions submitted to VADM Michael S. Rogers, USN, by Chairman Levin prior to the hearing with answers supplied follow:]

QUESTIONS AND RESPONSES

DEFENSE REFORMS

Question. The Goldwater-Nichols Department of Defense Reorganization Act of 1986 and the Special Operations reforms have strengthened the warfighting readiness of our Armed Forces. They have enhanced civilian control and clearly delineated the operational chain of command and the responsibilities and authorities of the combatant commanders, and the role of the Chairman of the Joint Chiefs of Staff. They have also clarified the responsibility of the Military Departments to recruit, organize, train, equip, and maintain forces for assignment to the combatant commanders.

Do you see the need for modifications of any Goldwater-Nichols Act provisions?

Answer. The integration of joint capabilities under the Goldwater-Nichols Act has been remarkable. All the warfighting benefits we enjoy from fighting as a joint force in air, land, sea—we are extending to cyberspace. In addition, it has improved civilian oversight of the Department of Defense (DOD) and fostered our military success over the last generation. Today U.S. military forces are more interoperable than ever before, and they set a standard for other militaries to attain. I see no need to modify the Goldwater-Nichols Act at this time.

Question. If so, what areas do you believe might be appropriate to address in these modifications?

Answer. I do not believe modifications to the Goldwater-Nichols Act are currently needed.

DUTIES

Question. What is your understanding of the duties and functions of the Commander, U.S. Cyber Command?

Answer. The Commander, U.S. Cyber Command (CYBERCOM) is responsible for executing the cyberspace missions specified in section 18.d.(3) of the Unified Command Plan (UCP) as delegated by the Commander, U.S. Strategic Command (STRATCOM) to secure our Nation's freedom of action in cyberspace and to help mitigate risks to our national security resulting from America's growing dependence on cyberspace. Subject to such delegation and in coordination with mission partners, specific missions include: directing Department of Defense Information Networks (DODIN) operations, securing and defending the DODIN; maintaining freedom of maneuver in cyberspace; executing full-spectrum military cyberspace operations; providing shared situational awareness of cyberspace operations, including indications and warning; integrating and synchronizing of cyberspace operations with combatant commands and other appropriate U.S. Government agencies tasked with defending our Nation's interests in cyberspace; provide support to civil authorities and international partners. All these efforts support DOD's overall missions in cyberspace of defending the Nation against cyber attacks, supporting the combatant commands, and defending DOD networks.

Question. What background and experience do you possess that you believe qualifies you to perform these duties?

Answer. I am humbled and deeply honored that the President has nominated me to be the 2nd Commander of CYBERCOM and the 17th Director of the National Security Agency (NSA). Over the past 3 decades, I have served in a wide variety of Joint and Navy positions that have prepared me well for the challenges ahead if confirmed by the U.S. Senate.

First, I have more than 32 years in the profession of arms, serving in various command, staff, and intelligence positions afloat and ashore. I have been the director for Intelligence for both the Joint Chiefs of Staff and U.S. Pacific Command, special assistant to the Chairman of the Joint Chiefs of Staff, and commanded at multiple levels. I have over 27 years of dedicated experience in the SIGINT arena as an In-

formation Warfare Officer and have held significant responsibilities in the cyber arena for much of the past 12 years.

In particular, my experiences and knowledge gained over the last 2½ years while serving as Commander of both Fleet Cyber Command and Tenth Fleet have done much to prepare me for the challenges of this new complex warfighting domain that is cyberspace. I should note that my responsibilities there include the command of the U.S. Navy's cryptologic capabilities, and so I have seen firsthand the relationship between cryptology and cybersecurity, and the importance of partnerships with interagency capabilities, with our allies, and with industry to strengthen the defense of our collective networks. My service at Fleet Cyber Command/Tenth Fleet afforded me direct experience, particularly in the realm of deliberate and crisis action planning, to ensure the effective execution of cyberspace responsibilities as directed by the Secretary of Defense through the Commander, STRATCOM.

Finally, my academic background has also helped prepare me for the challenges of high-level command, national security decisionmaking, and international engagement. I hold a Master of Science in National Security Strategy and am a graduate of both the National War College and the Naval War College. I was also a Massachusetts Institute of Technology Seminar XXI fellow.

Question. Does the Commander of CYBERCOM have command of or exercise operational control of the Defense Information Systems Agency's (DISA) and Military Services' communications networks?

Answer. If confirmed as Commander, CYBERCOM, I will be responsible for directing the operation and defense of DOD's information networks as specified in the UCP and as delegated by Commander, STRATCOM. The DISA provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to national leaders, joint warfighters, and other mission and coalition partners across the full spectrum of operations. As a Combat Support Agency, DISA maintains a close working relationship with CYBERCOM, providing expertise on the networks, communications and computing infrastructure that it operates. I will not exercise command or operational control over DISA communications networks.

Question. As a career intelligence officer, what qualifications do you have to command these networks?

Answer. As noted in my biography, much of my career has involved not only intelligence duties but the command, administration, use, and employment of information networks and the data they carry, process, and store to protect and guard our Nation. Over the course of my services, I have witnessed and helped further the revolution in information technology that has helped make our military second-to-none in its ability to communicate and control forces while providing decisionmakers with unprecedented situational awareness. I have also devoted a great deal of my service to understanding and mitigating the vulnerabilities that our dependence on information networks can create for our military and our Nation. In my current duties as Commander, Fleet Cyber Command I exercise operational control over Navy's networks and have done so for 30 months.

Question. What qualifications do you have to command military forces and military operations?

Answer. As noted above, I have exercised command previously at both junior and senior levels. I currently command Fleet Cyber Command and Tenth Fleet, a global team of nearly 15,000 men and women. Their operating environment is dynamic, and demanding; Fleet Cyber Command/Tenth Fleet has literally been "in action" against capable and determined adversaries seeking access to our networks since the day I assumed command in 2011. The planning and operations we have conducted to protect our networks and provide the Navy and our military and government freedom of maneuver in cyberspace have been complex.

Question. Do you believe that there are any steps that you need to take to enhance your expertise to perform the duties of the Commander, CYBERCOM?

Answer. Any individual can learn more to enhance his or her expertise and abilities, and I have found that truth amply applies to me in understanding the very complex and rapidly evolving domain that is cyberspace. If confirmed, I shall meet with the combatant commanders to ascertain how CYBERCOM can better support their missions. Additionally, I would engage with key officials and personnel within the executive and legislative branches of the U.S. Government, leaders throughout the Intelligence Community, Law Enforcement, the Department of Homeland Security (DHS), and senior allied officials to hear their ideas about how we can work together to identify, assess, and mitigate the cyber threats we all face.

RELATIONSHIPS

Question. Section 162(b) of title 10, U.S.C., provides that the chain of command runs from the President to the Secretary of Defense and from the Secretary of Defense to the commanders of the combatant commands. Other sections of law and traditional practice, however, establish important relationships outside the chain of command. Please describe your understanding of the relationship of the Commander, CYBERCOM, to the following officials:

The Secretary of Defense.

Answer. Pursuant to title 10, U.S.C., section 164, and subject to the direction of the President, the Commander, STRATCOM performs duties under the authority, direction, and control of the Secretary of Defense and is directly responsible to the Secretary for the preparedness of the command to carry out missions assigned to the command. As a sub-unified command under the authority, direction, and control of the Commander, STRATCOM, CYBERCOM is responsible to the Secretary of Defense through the Commander, STRATCOM. If confirmed, I will work closely with the Secretary in coordination with Commander, STRATCOM.

Question. The Deputy Secretary of Defense.

Answer. In accordance with title 10, U.S.C., section 132, the Deputy Secretary of Defense performs such duties and exercises powers prescribed by the Secretary of Defense. The Deputy Secretary of Defense will act for and exercise the powers of the Secretary of Defense when the Secretary is disabled or the office is vacant. If confirmed, I will work closely with the Deputy Secretary, in coordination with Commander, STRATCOM.

Question. The Director of National Intelligence.

Answer. The Intelligence Reform and Terrorist Prevention Act of 2004 established the Director of National Intelligence to act as the head of the Intelligence Community, principal advisor to the President and the National Security Council on intelligence matters pertaining to national security, and to oversee and direct the implementation of the National Intelligence Program. Pursuant to title 50, U.S.C., section 403, subject to the authority, direction, and control of the President, the Director of National Intelligence coordinates national intelligence priorities and facilitates information sharing across the Intelligence Community. If confirmed, I will work closely with the Commander, STRATCOM and through the Secretary of Defense to coordinate and exchange information with the Director of National Intelligence as needed to ensure unified effort and synergy within the Intelligence Community in matters of national security.

Question. The Under Secretary of Defense for Policy.

Answer. Title 10, U.S.C. and current DOD directives establish the Under Secretaries of Defense as the principal staff assistants and advisors to the Secretary of Defense regarding matters related to their respective functional areas. Within these areas, the Under Secretaries exercise policy and oversight functions, and in discharging their responsibilities, the Under Secretaries may issue instructions and directive memoranda that implement policy approved by the Secretary. If confirmed, I look forward to working with the Under Secretary of Defense for Policy, in coordination with Commander, STRATCOM, on all policy issues that affect CYBERCOM operations.

Question. The Under Secretary of Defense for Intelligence.

Answer. Title 10, U.S.C. and current DOD directives establish the Under Secretaries of Defense as the principal staff assistants and advisors to the Secretary of Defense regarding matters related to their respective functional areas. Within these areas, the Under Secretaries exercise policy and oversight functions and, in discharging their responsibilities the Under Secretaries may issue instructions and directive memoranda that implement policy approved by the Secretary. If confirmed, I shall work closely with the Under Secretary of Defense for Intelligence, in coordination with Commander, STRATCOM, on matters in the area of CYBERCOM's assigned responsibilities.

Question. The Under Secretary of Defense for Acquisition, Technology, and Logistics.

Answer. Title 10, U.S.C. and current DOD directives establish the Under Secretaries of Defense as the principal staff assistants and advisors to the Secretary of Defense regarding matters related to their respective functional areas. Within these areas, the Under Secretaries exercise policy and oversight functions and, in discharging their responsibilities the Under Secretaries may issue instructions and directive memoranda that implement policy approved by the Secretary. If confirmed, I shall work closely with the Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with Commander, STRATCOM, on matters in the area of CYBERCOM's assigned responsibilities.

Question. The Assistant Secretary of Defense for Homeland Defense.

Answer. The Assistant Secretary of Defense for Homeland Defense executes responsibilities including overall supervision of the homeland defense and defense support of civil authorities activities of the DOD while serving under the Under Secretary of Defense for Policy. Any relationship the Commander, CYBERCOM requires with the Assistant Secretary of Defense for Homeland Security would exist with and through the Under Secretary of Defense for Policy. If confirmed, I shall work with the Assistant Secretary of Defense for Homeland Defense in concert with Commander, STRATCOM; Commander, U.S. Northern Command; and Commander, U.S. Pacific Command, on related national security issues.

Question. The Chief Information Officer.

Answer. Under the authority of Department of Defense Directive 5144.02 and consistent with titles 10, 40, and 44, U.S.C., the DOD Chief Information Officer (CIO) is the Principal Staff Assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on information resources management and position, navigation, and timing matters. The DOD CIO is tasked with improving the combat power of the Department—as well as its security and efficiency—by ensuring that the Department treats information as a strategic asset and that innovative information capabilities are available throughout all areas of DOD supporting war fighting, business, and intelligence missions. The DOD CIO is the Department's primary authority for the policy and oversight of information resources management, to include matters related to information technology, network defense, and network operations, and it also exercises authority, direction, and control over the Director, DISA. If confirmed, I look forward to working closely with the Chief Information Officer through the Secretary and Deputy Secretary of Defense and Commander, STRATCOM, on matters in the area of CYBERCOM's assigned responsibilities.

Question. The Chairman of the Joint Chiefs of Staff.

Answer. The Chairman is the principal military advisor to the President, National Security Council, and Secretary of Defense. Title 10, U.S.C., section 163 allows communication between the President or the Secretary of Defense and the combatant commanders to flow through the Chairman. By custom and tradition, and as instructed by the UCP, if confirmed, I would normally communicate with the Chairman in coordination with the Commander, STRATCOM.

Question. The Secretaries of the Military Departments.

Answer. Under title 10, U.S.C., section 165, subject to the authority, direction, and control of the Secretary of Defense, and subject to the authority of the combatant commanders, the Secretaries of the Military Departments are responsible for administration and support of forces that are assigned to unified and specified commands. The authority exercised by a sub-unified combatant commander over Service components is clear but requires coordination with each Secretary to ensure there is no infringement upon those lawful responsibilities which a Secretary alone may discharge. If confirmed, I look forward to building a strong and productive relationship with each of the Secretaries of the Military Departments in partnership with Commander, STRATCOM.

Question. The Chiefs of Staff of the Services.

Answer. The Service Chiefs are charged to provide organized, trained, and equipped forces to be employed by combatant commanders in accomplishing their assigned missions. Additionally, these officers serve as members of the Joint Chiefs of Staff and as such have a lawful obligation to provide military advice. Individually and collectively, the Service Chiefs are a tremendous source of experience and judgment. If confirmed, I will work closely and confer regularly with the Service Chiefs.

Question. The combatant commanders and, specifically, the Commanders of STRATCOM and U.S. Northern Command.

Answer. CYBERCOM is a subordinate unified command under STRATCOM. The Commander, CYBERCOM, has both supported and supporting relationships with other combatant commanders, largely identified within the UCP, the Joint Strategic Capabilities Plan, execute orders, and operation orders. In general, the Commander, CYBERCOM, is the supported commander for planning, leading, and conducting DOD defensive cyber and global network operations and, in general, is a supporting commander for offensive missions. Specific relationships with Commander, U.S. Northern Command will be delineated by the President or the Secretary of Defense in execute and/or operation orders. If confirmed, I look forward to working with the combatant commanders to broaden and enhance the level and range of these relationships.

Question. The Director of the Defense Information Systems Agency.

Answer. The DISA is a DOD Combat Support Agency that provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to national leaders,

joint warfighters, and other mission and coalition partners across the full spectrum of operations. Commander, CYBERCOM must maintain a close relationship with the Director, DISA to coordinate and represent requirements in this mission area, in order to accomplish STRATCOM-delegated UCP missions. If confirmed, I shall work closely with the Director of DISA on matters of shared interest and importance.

OVERSIGHT

Question. The resourcing, planning, programming and budgeting, and oversight for CYBERCOM's missions is fragmented within the Defense Department, the executive branch as a whole, and within Congress. Section 932 of the National Defense Authorization Act (NDAA) for Fiscal Year 2014 requires the Secretary of Defense to appoint a Senate-confirmed official from the Office of the Under Secretary of Defense for Policy to act as the principal cyber advisor to the Secretary.

What is your view of this legislation? Do you believe that it will improve oversight, planning, and resource allocation for the cyber mission within DOD?

Answer. I believe this legislation provides an opportunity to streamline cyber policy analysis and oversight within DOD, and its implementation will support DOD's long-term goals in cyberspace. Cyber is a complex issue that touches many parts of the Department and one single point of contact within the Office of the Secretary of Defense will reduce duplicative efforts and keep all offices that work on cyber issues in sync.

Question. What changes to the legislation, if any, would you recommend?

Answer. I do not recommend any changes at this time. If confirmed, I can assure you that I will work closely with the principal cyber advisor selected by the Secretary of Defense.

MAJOR CHALLENGES AND PROBLEMS

Question. In your view, what are the major challenges that will confront the Commander, CYBERCOM?

Answer. I believe the major challenge that will confront the next Commander, CYBERCOM, will be dealing with the changing threat in cyberspace. Adversaries today seek persistent presences on military, government, and private networks for purposes such as exploitation and potentially disruption. We as a military and a nation are not well positioned to deal with such threats. These intruders have to be located, blocked, and extracted, sometimes over long periods of time. We have seen the extent of the resources required to wage such campaigns, the planning and intelligence that are essential to their success, and the degree of collaboration and synchronization required across the government and industry (and with our allies and international partners). We in DOD are creating capabilities that can adapt to these uses and others, but we have some key capability gaps in dealing with increasingly capable threats. Our legacy information architecture, for instance, is not optimized for defense in its current form, and our communications systems are vulnerable. U.S. military forces currently lack the training and the readiness to confront advanced threats in cyberspace. Finally, our commanders do not always know when they are accepting risk from cyber vulnerabilities, and cannot gain reliable situational awareness, neither globally nor in U.S. military systems.

Question. Assuming you are confirmed, what plans do you have for addressing these challenges?

Answer. If confirmed, I plan to continue CYBERCOM's current course of building cyber capabilities to be employed by senior decisionmakers and combatant commanders. In accordance with the DOD Strategy for Operating in Cyberspace, CYBERCOM with its mission partners and allies has been helping the DOD to build:

1. A defensible architecture;
2. Trained and ready cyber forces;
3. Global situational awareness and a common operating picture;
4. Authorities that enable action;
5. Doctrine and concepts for operating in cyberspace.

I would plan to assess these current priorities, which are DOD-wide, with an eye to shifting emphases across them as necessary and appropriate, and as computer and communication technologies continue to evolve.

Question. What are your priorities for the CYBERCOM?

Answer. CYBERCOM is helping to accomplish something that our military has never done before. With the Services, allies, and a host of partners, it is putting in place foundational systems and processes for organizing, training, equipping, and operating military cyber capabilities to meet cyber threats. CYBERCOM and the

Services are building a world class, professional, and highly capable force in readiness to conduct full spectrum cyberspace operations. Its Cyber Mission Force (CMF) is already engaged in operations and accomplishing high-value missions. It is no longer an idea on a set of briefing slides; its personnel are flesh-and-blood soldiers, marines, sailors, airmen, and coastguardsmen, arranged in military units. That progress is transforming potential capability into a reliable source of options for our decisionmakers to employ in defending our Nation. Future progress in doing so, of course, will depend on our ability to field sufficient trained, certified, and ready forces with the right tools and networks to fulfill the growing cyber requirements of national leaders and joint military commanders. If confirmed, my highest priority will be continuing and expanding this progress toward making CYBERCOM capable of protecting our Nation's freedom of maneuver in cyberspace.

THE FUNDAMENTAL PROSPECTS FOR DEFENDING AGAINST CYBER ATTACKS

Question. The ease with which nation-states, terrorists, and criminals, are able to penetrate corporations and government organizations to steal information suggests that the prospects for cyberdefense, using current techniques at least, are poor. Nonetheless, CYBERCOM has been assigned the mission of defending the Homeland, which at least implies that a defensive mission is practical and achievable. It may be possible to build resilience into critical infrastructure to recover from an attack, through back-up systems and redundant control systems that are less automated or electronically connected, but the Government so far has not emphasized resilience over defense for our most critical infrastructure.

On a sustained basis in a conflict with a very capable nation-state, should we expect CYBERCOM to be able to prevent cyber attacks from reaching their targets or causing great damage?

Answer. The United States possesses superior military might across all warfighting domains, cyberspace included. In truth, however, there has been no large scale cyber conflict yet in history, and the state of strategy and execution of cyber warfare is evolving as we speak. Our decision to collocate key intelligence operations and cyberspace capability serves as a force multiplier, if properly authorized and supported by policy, resources, and willpower. Our force construct is such that it provides the United States the flexibility to engage, both offensively and defensively, in specific areas of hostility or on a transnational basis. We are building or further developing our international partnerships and relationships for mutual support and recognition of norms of behavior. We know there are other nation-states who have equal or near-equal capability to ours; we have to be sure that we have the capabilities, processes, authorities, and, where appropriate, delegation and preapprovals in place to prevent and respond to malicious activity. In a conflict where risk to our systems, information, and critical infrastructure was in play, that the United States would need to optimize our ability to see, block, and maneuver against attackers in a streamlined and efficient fashion. We still have significant work to do to build out our forces and capabilities. However, given the circumstances, yes, I believe it is realistic to expect that U.S. CYBERCOM could effectively engage the adversary to prevent attacks and severe damage.

Question. Is it reasonable to expect the private sector nonetheless to build defenses to prevent serious impacts on critical infrastructure?

Answer. Yes. I believe that mission assurance and the protection of our critical infrastructure is an inherent obligation of all, not just DOD, DHS, DOJ/Federal Bureau of Investigation (FBI) and our Government. In many cases, mission assurance relies on the provision, management, or facilitation of critical infrastructure lies in the private sector. Defensive measures could include not just automated capabilities to prevent or respond, but also adherence to proper standards of network security, administration, sharing of threat and vulnerability information, and compliance. These are as critical to protection of infrastructure as is military or cyber might. In almost any scenario, collaboration and information sharing across private and public, governmental and non-governmental organizations will be a key to successful outcomes.

Question. In your view, could such cyber attacks be prevented through the development of offensive capabilities and the principles of deterrence?

Answer. Yes, the development of both offensive and defensive capabilities can serve to deter an adversary from cyber attack. Strong capabilities can deter an attack by preventing an adversary from achieving his objectives and demonstrating the ability to impose costs on the adversary.

Question. Should we expect CYBERCOM to be able to prevent the more limited attacks that could be expected from powers with lesser cyber capabilities, such as North Korea and Iran?

Answer. Adversarial activities over recent years have shown that the level of expertise required to conduct potentially damaging operations has steadily lowered, enabling less capable actors to achieve some level of effect. Although we continue to build and develop our forces and capabilities, I believe that CYBERCOM has the capability to prevent such attacks, yes, whether from a capable or less capable adversary, given the order and provided that the supporting policies, authorities, relationships, and will to act are in place.

Question. In your view, can cyber warfare capabilities provide an asymmetric advantage for such rogue nations, providing them the potential to strike the American people and economy?

Answer. Yes. Regardless of the target—assuming that the adversary has somehow developed the access—the physics of the cyberspace domain and the technology supporting it make it easier for an adversary to hide or obfuscate his capability, attack vector, and location, and deliver an effect on his target either singularly or repeatedly within milliseconds. If he or she has subverted any number of proxies from which to operate, that further multiplies the advantage enjoyed. When the victim is placed in a reactive posture by processes which constrain the ability to respond, the advantage is multiplied. Internal defensive measures can mitigate that advantage to an extent, of course.

Question. If so, how should we demonstrate or clarify our retaliatory capability as a means of contributing to deterrence? Should the U.S. Government be more forthcoming about the nature of cyber warfare, and the balance between offensive and defensive capabilities?

Answer. I believe the recent disclosures of a large portion of our intelligence and military operational history may provide us with opportunity to engage both the American public and our international partners in discussion of the balance of offense and defense, the nature of cyber warfare, norms of accepted and unacceptable behavior in cyberspace, and so forth.

SUPPORT TO CIVIL AUTHORITIES

Question. CYBERCOM has a mission to support civil authorities, such as DHS and law enforcement agencies, to help defend government networks and critical infrastructure networks owned and operated by the private sector.

Please describe the ways that CYBERCOM should assist civil authorities and the capability of CYBERCOM to provide that assistance.

Answer. I believe that a request for support to civil authorities for cyber related assistance normally occur as a response to a request for assistance from DHS to DOD, and in close coordination with the Commanders of STRATCOM and NORTHCOM. That support could be technical assistance in a number of different ways, such as recommendations for improved network configurations, information assurance measures, or specific defensive response actions. Other technical assistance could be in the form of mitigation options, forensics, or data analysis.

Question. U.S. Northern Command was established to serve as the focal point for DOD support to civil authorities.

Will cybersecurity support to civil authorities be provided through U.S. Northern Command, as a supported command, or otherwise? If not, why not?

Answer. Depending on the nature of the national emergency or crisis, and the requirement for cybersecurity support, the Secretary of Defense would determine which combatant commander would be supported and supporting and CYBERCOM would comply with that determination. In any scenario with respect to cyber security support to civil authorities, a close collaborative relationship between U.S. Northern Command and CYBERCOM will be key.

USE OF FORCE IN CYBERSPACE

Question. Does the Defense Department have a definition for what constitutes use of force in cyberspace, and will that definition be the same for our activities in cyberspace and those of other nations?

Answer. DOD has a set of criteria that it uses to assess cyberspace events. As individual events may vary greatly from each other, each event will be assessed on a case-by-case basis. While the criteria we use to assess events are classified for operational security purposes, generally speaking, DOD analyzes whether the proximate consequences of a cyberspace event are similar to those produced by kinetic weapons.

As a matter of law, DOD believes that what constitutes a use of force in cyberspace is the same for all nations, and that our activities in cyberspace would be governed by Article 2(4) of the U.N. Charter the same way that other nations would be. With that said, there is no international consensus on the precise definition of

a use of force, in or out of cyberspace. Thus, it is likely that other nations will assert and apply different definitions and thresholds for what constitutes a use a force in cyberspace, and will continue to do so for the foreseeable future.

Question. Has the Defense Department, or the administration as a whole, determined what constitutes use of force in cyberspace in relation to the War Powers Act, the exercise of the right of self-defense under the U.N. Charter, and the triggering of collective defense obligations?

Answer. It is up to the President to determine when, based upon the circumstances of any event, including a cyberspace event, and the contemplated response that the President intends to proceed with, what consultations and reports are necessary to Congress, consistent with the War Powers Act.

The United States would evaluate its individual self-defense rights, as well as the self-defense rights of other nations, consistent with international law and Article 51 of the U.N. Charter. This analysis would assess whether an illegal use of force had occurred, and whether a State's inherent right of self-defense was triggered. If the United States held a collective defense obligation to the state that was subject to the illegal use of force, then the United States would evaluate its obligations consistent with its treaty obligations, keeping in mind that the U.N. Charter recognizes a state's inherent right of individual and collective self-defense. After all, collective self-defense obligations apply when another state is threatened or subject to a use of force in the cyber domain just as they would in other warfighting domains.

Question. Could CYBERCOM employ offensive cyber weapons against computers located abroad that have been determined to be sources of an attack on the United States or U.S. deployed forces if we do not know who is behind the attack (i.e., a foreign government or non-state actors)? Without confident "attribution," under international law, would the Defense Department have the authority to "fire back" without first asking the host government to deal with the attack?

Answer. International law does not require that a nation know who is responsible for conducting an armed attack before using capabilities to defend themselves from that attack. With that said, from both an operational and policy perspective, it is difficult to develop an effective response without a degree of confidence in attribution. Likely, we would take mitigating actions, which we felt were necessary and proportionate, to defend the Nation from such an attack. I'd note that in such an event, CYBERCOM would be employing cyber capabilities defensively, in the context of self-defense.

POLICIES GOVERNING ACCESS TO SENSITIVE TARGETS FOR INTELLIGENCE COLLECTION AND TARGETING

Question. Traditionally, espionage has not been regarded as a use of force or an act of war. However, in cyberspace operations, experts agree that gaining access to a target for intelligence collection is tantamount to gaining the ability to attack that target. If a penetration were detected, the victim may not know whether the purpose of the activity would be limited to espionage only, or would also constitute preparation for an attack.

Are there classes of foreign targets that the U.S. Government considers should be "off-limits" from penetration through cyberspace?

Answer. My view is that the U.S. Government should only conduct cyberspace operations against carefully selected foreign targets that are critical to addressing explicitly stated intelligence and military requirements, as approved by national policymakers and the national command authority.

Question. Would or should such targets be immune to penetration by the United States in peacetime even for intelligence collection? Should there be a review process outside of DOD for such potential targets?

Answer. Intelligence collection is conducted in response to specific needs expressed by policymakers and military commanders for information. Those needs are vetted through a formal requirements process managed by the Director of National Intelligence that includes a review of sensitive policy equities.

Question. How does the NSA currently consider these issues when making decisions about targeting for intelligence collection?

Answer. NSA conducts intelligence collection operations in response to specific requirements that are vetted through a formal process managed by the Director of National Intelligence. That process includes an interagency review of sensitive policy equities.

Question. What role do the White House and the interagency coordination process play in this decision process?

Answer. The White House and the interagency community are directly involved in approving foreign intelligence requirements and determining what targets are ap-

propriate for cyberspace and other Signals Intelligence (SIGINT) operations. All cyberspace operations conducted by NSA and CYBERCOM are governed by the policy constraints set by the White House and the interagency coordination process. President Obama recently announced improvements to this process in Presidential Policy Directive PPD–28.

NSA and CYBERCOM (under its delegated intelligence authorities) conduct intelligence collection operations in response to specific requirements that are vetted through a formal process managed by the Director of National Intelligence. That process includes an interagency review of sensitive policy equities.

Question. Do you see a need for a change in the decisionmaking process?

Answer. I believe that the recent improvements to the policy review process described in PPD–28 should be sufficient to ensure that all U.S. Government and privacy interests are considered prior to engaging in cyberspace operations. I have no specific recommendations for additional changes at this time.

AUTHORITIES OF COMMANDER, U.S. CYBER COMMAND

Question. Offensive cyber warfare weapons or operations could have devastating effects, depending on the target of the attack and the method used, that could be comparable to those caused by weapons of mass destruction.

Under what circumstances, if any, would you as Commander, CYBERCOM, have the authority to use offensive cyber weapons without prior approval by the President?

Answer. Under current policy, Commander, CYBERCOM, would not use cyber capabilities for offensive purposes without prior approval by the President.

Question. Are CYBERCOM forces the only forces permitted to conduct offensive military cyber operations?

Answer. The President or Secretary of Defense could authorize any combatant command to direct assigned cyber forces to conduct military cyberspace operations. At present, we are building a CMF, which will be able to conduct these operations under the command and control of whichever combatant command to which they are assigned.

Question. Are there official rules barring non-CYBERCOM forces from, for example, causing cyber effects against battlefield weapons systems, as an extension of traditional electronic warfare capabilities?

Answer. As far as I am aware, there are none.

Question. Are there clear distinctions between cyber warfare and electronic warfare?

Answer. While there are clear distinctions between electronic warfare and cyber warfare, there may also be avenues to achieve greater operational synergy between these two missions and to examine the policy implications of their synchronized use in warfare.

LAWS OF WAR

Question. Has DOD determined how the laws of armed conflict (including the principles of military necessity in choosing targets, proportionality with respect to collateral damage and unintended consequences, and distinguishing between combatants and non-combatants) apply to cyber warfare, with respect to both nation-states and non-state entities (terrorists, criminals), and both when the source of an attack is known and unknown?

Answer. Per DOD guidance, all military operations must be in compliance with the laws of armed conflict—this includes cyber operations. The law of war principles of military necessity, proportionality and distinction will apply when conducting cyber operations.

Question. If not, when will the Department produce authoritative positions on these issues?

Answer. N/A.

EQUITIES

Question. There have been many instances in history where military and political leaders had to struggle with the choice of acting on intelligence information to save lives or forestall an enemy success, but at the cost of the enemy learning that their classified information or capabilities had been compromised. These choices are referred to as "balancing equities" or "gain-loss" calculations.

Who is in charge of the equities/gain-loss process for cyberspace within the military?

Answer. There is a clear framework established to adjudicate the equities/gain-loss and is part of both crisis and deliberate planning efforts on the part of the com-

batant commanders. The risk-loss equation in DOD is made after comprehensive consultation with the Intelligence Community and the impacted commander. CYBERCOM is the lead for DOD cyberspace deconfliction and is directly involved in cases of disagreement as part of the processes directed in key interagency documents. If the interagency disagreement is not resolved at this level, the issue goes to the Chairman, Joint Chiefs of Staff, the Secretary of Defense, NSC Deputies, and later to the President where the issue is resolved.

Question. If these decisions rest with the Commander of CYBERCOM, how will the combatant commands, the military Services, and other defense agencies be persuaded that their interests will be fairly balanced with those of NSA?

Answer. PPD–20 allows for representation from other agencies, giving each a voice in the process. When gain-loss issues arise, all parties have the responsibility to comprehensively state the issues and impacts with these discussions beginning at the action officer level. Formal disagreements unresolved after CYBERCOM review follow a clear path to department and national decisionmakers, to include the President if need be.

Question. Since NSA personnel are filling a large number of key positions within CYBERCOM, how can you be confident that equity issues make it to senior levels in CYBERCOM, and are fully and fairly examined?

Answer. The value of NSA's contribution to the CYBERCOM mission in terms of manpower and mission support is vitally important; however, I believe that the military and civilian personnel in the current CYBERCOM workforce contains a broad mix of experience and background from across the defense, intelligence, operations and law enforcement communities. Within the intelligence directorate for example, the Defense Intelligence Agency is the primary provider of personnel, with a senior executive from that agency holding the deputy director position. Staffing the leadership from a wide range of sources is a strength that has resulted in a more diverse level of input into the equities process than ever before. All issues requiring senior leadership attention are fully and fairly vetted through a rigorous system of boards and working groups, made up of representation from across our diverse leadership cadre.

Question. How are equities/gain-loss decisions made for the Nation as a whole? How will the interests of the vulnerable private sector, critical infrastructure, and civil agencies be weighed in the selection of targets for intelligence collection and attack?

Answer. The Tri-lateral Memorandum of Agreement contains a deconfliction mechanism involving DOD, DOJ, the Intelligence Community and agencies outlined in, and reinforced by PPD–20. Disagreements are handled similar to those internal to DOD; the issue is forwarded from the Seniors involved to the Deputies then on to the Principals Committee with the final stop being the President in cases where equities/gain-loss are ultimately resolved.

Question. As a foreign intelligence agency, NSA has a mission to find vulnerabilities in the networks of our adversaries. However, the NSA's Information Assurance Directorate is responsible for securing national security systems and CYBERCOM has the responsibility of defending DOD networks and the Nation.

How do you believe these responsibilities should be balanced?

Answer. The basis for handling discovered vulnerabilities must be the national interests of the United States. Understanding particular vulnerabilities, and how they may impact our national interests, requires deep understanding of the technology, the risks a vulnerability can pose, options for mitigating these risks, and the potential for foreign intelligence if the vulnerability remains open. But the balance must be tipped toward mitigating any serious risks posed to the U.S. and allied networks. NSA has always employed this principle in the adjudication of vulnerability findings, and if confirmed, I intend to sustain the emphasis on risk mitigation and defense.

Question. What are the policies and processes that apply to the discovery and disclosure of so-called "0-day" vulnerabilities in software?

Answer. Within NSA, there is a mature and efficient equities resolution process for handling "0-day" vulnerabilities discovered in any commercial product or system (not just software) utilized by the United States and its allies. The basis for it is documented in formal NSA policy, which includes the adjudication process. The policy and process ensure that all vulnerabilities discovered by NSA in the conduct of its lawful missions are documented, subject to full analysis, and acted upon promptly.

NSA is now working with the White House to put into place an interagency process for adjudication of 0-day vulnerabilities. If confirmed, I will support this process.

Question. What is the impact of not disclosing these vulnerabilities? What is the impact of disclosing them?

Answer. When NSA discloses a vulnerability discovery to a vendor, the goal is to achieve the most efficient and comprehensive mitigation of the risk. Upon disclosure, vendors usually fix the vulnerability, and issue an update or patch. The risk is mitigated only when users actually install the patch. Since adversaries frequently study industry patches to learn about underlying vulnerabilities that will remain in unpatched systems, NSA disclosure of a vulnerability may temporarily increase the risk to U.S. systems, until the appropriate patches are installed.

When NSA decides to withhold a vulnerability for purposes of foreign intelligence, then the process of mitigating risks to U.S. and allied systems is more complex. NSA will attempt to find other ways to mitigate the risks to national security systems and other U.S. systems, working with stakeholders like CYBERCOM, DISA, DHS, and others, or by issuing guidance which mitigates the risk. If confirmed, I intend to strengthen collaboration with other Government stakeholders, under the auspices of the planned interagency process.

Question. What is the impact of not disclosing these vulnerabilities? What is the impact of disclosing them?

Answer. NSA currently follows its equity resolution process, as required under NSA policy. Technical experts document the vulnerability in full classified detail, options to mitigate the vulnerability, and a proposal for how to disclose it. The default is to disclose vulnerabilities in products and systems used by the United States and its allies. The information assurance and intelligence elements of NSA jointly participate in this process.

DETERRENCE AND ESCALATION CONTROL

Question. Does the U.S. Government have a cyber warfare deterrence strategy or doctrine?

Answer. Deterrence in cyberspace is achieved through the totality of U.S. actions, including the United States overall defense posture and the resilience of our networks and systems. As the President stated in his International Strategy for Cyberspace, the United States reserves the right to defend itself against cyberattacks. Whenever possible, the United States will exhaust all options prior to military force, and will always act in accordance with U.S. values and in a manner consistent with the Constitution and international law. This administration has articulated these policies consistently since the International Strategy for Cyberspace was published in 2011. The establishment of CYBERCOM is an element of a deterrence strategy, but more work and planning will be required to evolve a solid national strategy.

Cyber warfare is a complex and evolving discipline, and the subject of deterrence is drawing increasing attention at all levels of government and the Interagency, and in our discussions with our international partners. If confirmed, I will work with DOD, DHS, DOJ/FBI and others as we work to establish the relationships and engagement necessary to build such a strategy and policy.

Question. Would you agree that promulgating such a doctrine requires at least some broad statements of capabilities and intentions regarding the use of offensive cyber capabilities, both to influence potential adversaries and to reassure allies?

Answer. Classic deterrence theory is based on the concepts of threat and cost; either there is a fear of reprisal, or a belief that an attack is too hard or too expensive. Cyber warfare is still evolving and much work remains to establish agreed upon norms of behavior, thresholds for action, and other dynamics. A broad understanding of cyber capability, both defensive and offensive, along with an understanding of thresholds and intentions would seem to be logical elements of a deterrence strategy, both for our allies and our adversaries and as they are in other warfighting domains. I believe we'll see much discussion of the structure and implementation of our cyber deterrence strategy from DOD and Intelligence Community experts, along with Interagency engagement.

Question. How do you reconcile the utility of speaking more openly and candidly about cyber warfare capabilities in the interest of promoting greater public knowledge and the development of deterrence doctrine with the continued need to classify U.S. cyber capabilities?

Answer. I believe that as we communicate more with the public, the understanding that the United States will defend and deter in cyberspace, in accordance with law and international agreement, is more important than understanding the intricacies of the capabilities it will use to do so. I believe the public will understand that we do not want to telegraph our strategy for action to the adversary. As cyberspace matures as a warfighting domain, I believe our classification policies will also evolve to support growing domestic and international partnerships and relationships. Regardless, we will adhere with all classification policies and practices dictated by Executive order.

Question. Most experts believe that the attacker has a substantial advantage over the defender in cyber warfare. It is also widely believed that striking first against an adversary's networks offers an advantage if the adversary's command and control networks can be degraded, and because the attacker can take steps to protect itself from a retaliatory attack. These considerations suggest that cyber warfare is currently "unstable" from the perspective of classic deterrence theory and escalation control.

What are your views of these dynamics?

Answer. There is no doubt that the dynamics of offense and defense in cyberspace are complex, simply due to the physics of the engagement space. Automated capabilities, human response cycles, and many other factors make them even more so. These considerations are discussed and debated by experts across the whole of government, industry, and academia on a near-constant basis. The science and the philosophy are evolving. Just as it took time for doctrine, strategy, and concepts of deterrence and escalation to evolve in the other warfighting domains, so it is with cyber warfare. I believe we are making progress.

IMPLICATIONS OF U.S. DEPENDENCE ON CYBER NETWORKS

Question. Many experts assert that the United States is the most vulnerable country in the world to cyber attack because we are the most networked nation and the one that has most fully exploited computer networks for business, government, and military functions.

How could the Department compensate for U.S. dependence on vulnerable cyber networks in developing effective deterrent strategies?

Answer. We have effective deterrent strategies in place in the other warfighting domains, in the form of our demonstrated military might and capability. Cyber deterrence should evolve in the same way; demonstrated capability to defend, respond, or be able to attack when necessary is a key to deterrence. Our dependence on our networks can be compensated for by having a strong, viable defense in the form of both traditional military strength and cyber capability. We have the ability to respond proportionately and discriminately in both kinetic and non-kinetic modes when we can meet attribution requirements.

We need, however, to move from what is currently a reactive posture, to a proactive one. We are integrating and synchronizing our military operations and supporting intelligence capabilities for optimal detection, analysis, assessment, and response to mitigate threats and vulnerabilities on a near real-time basis. The concepts we are maturing in the form of multi-layered approaches and scalability, in coordination with DHS and others, are expandable to the rest of our Government and critical infrastructure.

Our networks are inherent to our way of life; their vulnerability is the key concern. A strong and deterrent defense, along with robust, resilient networks, will alleviate that vulnerability.

Question. Given our vulnerabilities, is it in our interest to avoid engaging in certain kinds of offensive cyber warfare—so that we do not set precedents by example for others to follow?

Answer. Any decision to engage in offensive cyber operations must reflect careful consideration and due diligence of the range of potential impacts, including adversary responses and the impact upon norms and precedents in cyberspace. Even as we must be prepared to undertake offensive cyber operations, these are important considerations in the decision to undertake such operations.

THE CHALLENGE OF ATTRIBUTION

Question. An essential feature of military, intelligence, and criminal or malicious activities in cyberspace is the ease with which the origin and the identity of those responsible for an attack can be concealed—the problem of "attribution".

Can deterrence be an effective strategy in the absence of reliable attribution?

Answer. Yes, I believe there can be effective levels of deterrence despite the challenges of attribution. Attribution has improved, but is still not timely in many circumstances. We must employ several approaches to this challenge. A healthy, engaged partnership with the Intelligence Community is vital to continued improvement in attribution. Second, is development of defensive options which do not require full attribution to meet the requirements of law and international agreement. Cyber presence, being forward deployed in cyberspace, and garnering the indications and warnings of our most likely adversaries can help (as we do with our forces dedicated to Defend the Nation). We must ensure we leverage the newest technology to identify our attackers before and during an attack—not just after. Last, and perhaps most important, we need to make our networks and supporting architectures robust,

resilient, and defensible by establishing and encouraging adherence to cybersecurity and information assurance standards. This last is a national problem across all of our networks, and is one which we should actively work to resolve.

There are other actions that need to be taken, too, in order to advance our defensive capability and support a deterrent posture. These include partnerships with nation-states who share common goals and expectations for behavior in cyberspace. From these partnerships, we can build normative standards, thresholds for action, and evidential frameworks on which to base response. We also need to improve our relationships with private and industrial sector partners through information sharing regarding threat and vulnerabilities.

I believe the United States may be considered an easier mark because our own processes and criteria for response lead the adversary to believe, rightly or wrongly, that we do not have the will to respond in a timely or proportionate manner, even when attribution is available. This is within our capacity to fix.

The bottom-line is that we have much we can do to increase our posture to prevent attacks, mitigate them to at least a reasonable extent, or deter them outright, without full attribution.

Question. Can the attribution problem be solved without comprehensive information sharing among the private sector and with the government?

Answer. I believe that the difficulty of attribution is compounded without a close relationship with the private sector, and full information sharing to the degree that policy and law allow. Most of our national information systems and networks ride on or are composed of infrastructure that is privately owned; we need their engagement to build attribution capability.

SYSTEMS ACQUISITION

Question. Combatant commands by design play a limited role in the acquisition process. However, the Commander of CYBERCOM is dual-hatted as the Director of the NSA, which is a large enterprise with substantial resources for developing, procuring, and supporting new equipment, systems, and capabilities. In addition, the Commander exercises operational control of DISA networks, and DISA is also an agency that acquires systems and capabilities.

Is there a precedent for a combatant commander to exercise this degree of direct control over acquisition organizations, aside from Special Operations Command, which Congress expressly provided with acquisition authority?

Answer. If confirmed as the Commander, CYBERCOM, I will rely upon the acquisition authority of other organizations, (e.g., the Services and Defense Agencies) to equip the cyber forces to satisfy validated operational requirements and comply with DOD policy and capability development guidance. This is the same process used by the other combatant and sub-unified commands, with the exception of U.S. Special Operations Command.

Question. What measures have been taken to ensure that Commanders of CYBERCOM do not circumvent the requirements process and the established acquisition process by directing subordinates at NSA or DISA to directly address needs perceived by CYBERCOM without the rigor required by the DOD requirements and acquisition processes?

Answer. CYBERCOM, NSA, and DISA are all separate organizations with their own, ability to acquire personnel and equipment, processes and staffs. Due to the separate nature of these three organizations, the oversight, accountability chains, and the ability to audit will ensure I follow the CYBERCOM requirements process and the Director of NSA follows the established NSA acquisition process. As mentioned earlier, CYBERCOM will operate under the same authorities and oversight as other combatant commands and sub-unified commands.

Specifically regarding rigor, CYBERCOM adheres to all laws and policies regarding acquisition and if confirmed, I will ensure DOD requirements and acquisition processes will continue to be followed.

Specifically, I understand the Department directed CYBERCOM to establish the DOD Cyber Operational Capabilities Board (COCB) to better integrate military cyber capabilities requirements into cyber capability development. The COCB is in its infancy and the draft Charter is still being staffed, but it will be fully alignment with the Department's Joint Capabilities Integration and Development System to ensure future cyberspace capability development supports the Combatant Commands.

It is important to note that although CYBERCOM, as a sub-unified command, does not have its own acquisition authority, it has the management controls necessary to ensure Command activities for funding capability developments satisfy validated operational requirements and comply with DOD policy and capability de-

velopment guidance. While CYBERCOM does not have the acquisition authority to designate a Milestone Decision Authority (MDA), the Command makes investment decisions that result in starting, continuing, suspending, or terminating its investments in cyberspace capability developments. These decisions are made in concert with executing MDAs and reflect the Command's focus on funding only those capability developments that will deliver required operational cyberspace capabilities within the timeframes needed. As discussed previously, CYBERCOM will rely upon the acquisition authority of other organizations, e.g., the Services and Defense Agencies.

Question. The NDAA for Fiscal Year 2011 required the Secretary of Defense to establish a strategy for streamlining the acquisition and oversight process for cyber warfare capabilities, which resulted, among other things, in the establishment of the Cyber Investment Management Board (CIMB).

Three years after the passage of this legislation, how would you characterize DOD's progress in establishing an agile acquisition process to provide capabilities for CYBERCOM?

Answer. The CIMB was established in 2012 and has been meeting on a quarterly basis. The CIMB is chartered to provide strategic guidance and recommendations to support integration and synchronization of cyber capabilities across science and technology requirements, acquisitions, development, test and evaluation, and sustainment to ensure that cyber warfare investments are efficiently planned, executed, and coordinated across the Department. The CIMB continues to mature and is working to demonstrate a streamlined acquisition and oversight process for cyber warfare capabilities. Currently, they have identified pilot programs to demonstrate the proof of principle for rapid acquisition of cyber capabilities.

MILITARY SERVICE ROLES IN U.S. CYBER COMMAND

Question. Each of the Military Services is producing cyber operations units for assignment to CYBERCOM to defend the Nation, support the other combatant commands, and to defend DOD networks.

Are these Army, Navy, Marine Corps, and Air Force units geographically organized and assigned, or is there also specialization among the Military Services by mission or type of target?

Answer. Service provided CMF Teams are both geographically aligned and specialized depending upon their assigned mission area.

The Cyber National Mission Force is comprised of National Mission Teams, National Support Teams, and National Cyber Protection Teams. They are assigned to the "Defend the Nation" in cyberspace mission area and, if directed, defend our critical infrastructure and key resources against nation state and non-state actors.

The Combat Mission Forces are comprised of Combat Mission Teams and Combat Support Teams. They are assigned to the "Provide Support to Combatant Commands" mission area. Combat Mission Forces are geographically and functionally aligned under one of four Joint Force Headquarters-Cyber (JFHQ–C) in direct support of geographic and functional combatant commands. They are aligned as follows:

- JFHQ–C Washington supports U.S. Special Operations Command, U.S. Pacific Command, and U.S. Southern Command
- JFHQ–C Georgia supports U.S. Central Command, U.S. Africa Command, and U.S. Northern Command
- JFHQ–C Texas supports U.S. European Command, STRATCOM, and U.S. Transportation Command

The Combat Protection Forces are comprised of Service, DISA, and Combatant Command Cyber Protection Teams. They are assigned to the "Secure, Operate, and Defend the Department of Defense Information Networks" mission area. These teams are specialized to prepare and protect key cyber terrain to provide mission assurance.

Question. Would, for example, Army units be assigned to operate against naval or air targets, and vice versa?

Answer. Yes, targets developed for fires and effects delivered in and through cyberspace do not necessarily correspond with traditional Service domains much as an Air Force unit may be tasked to attack a naval vessel. The cyberspace domain often intersects with multiple elements of a single target. A Target System Analysis that yields multiple aimpoints provides a commander flexibility on how best to prosecute the target with the least risk. These options may require an Army unit to operate against naval or air targets and vice versa. Ultimately, the Joint Force Commander will determine how best to engage a target with the cyber mission forces at his/her disposal.

Question. Will each geographic combatant command have a mix of units from each Military Service?

Answer. Each geographic combatant command is supported by a Joint Force Headquarters-Cyber with personnel from all Services, and with the exception of U.S. Africa Command, all GCCs have a combination of Service established CMF teams aligned. Currently, all U.S. Africa Command CMFs are U.S. Army provisioned.

Question. Will geographic combatant commanders be permitted to execute cyber operations under their own authorities?

Answer. Geographic combatant commanders already have authority to direct and execute certain Defensive Cyberspace Operations (DCO) within their own networks. These actions consist of internal defensive measures to prepare and protect mission critical networks. In the event of hostilities or contingency operations, combatant commanders would be permitted to execute full spectrum cyber operations as approved by the President and directed by the Secretary of Defense.

FOCUS ON INTELLIGENCE GATHERING VERSUS FOCUS ON WARFIGHTING

Question. The NSA, as an intelligence agency, appropriately places the highest importance on remaining undetected, and accordingly invests in high-end—and therefore expensive and hard-to-develop—technical tools and tradecraft, following a deliberate methodology for developing and maintaining capability. CYBERCOM, as a military combatant command, has very different interests and objectives. For example, it must have the capability to act rapidly, it may need tools and processes that do not require computer scientists to operate them, and it may need to act in a fashion that makes it clear that the operation is an attack by the United States.

Do you believe that you could direct CYBERCOM wartime operations effectively if CYBERCOM were only able to use the NSA infrastructure to support those operations?

Answer. It depends. We must ensure we have the tools and infrastructure needed to accomplish our mission whenever necessary. CYBERCOM should leverage the NSA platform where appropriate and cost-effective, while developing additional infrastructure to accomplish military operations that are unique and distinguishable from the Intelligence Community.

Question. How scalable are NSA infrastructure, personnel, and tools for supporting combat operations in cyberspace?

Answer. NSA's infrastructure and tools could be scaled to support combat operations in cyberspace. To most effectively manage risks across military and intelligence operations in cyberspace, CYBERCOM and the Services need to leverage NSA expertise to build cyberspace capabilities for combat operations which could include additional tools and infrastructure that are unique and distinguishable from the Intelligence Community.

Question. On what schedule should CYBERCOM develop the capability to take offensive actions that do not require hiding the fact that the operations are being conducted by U.S. forces?

Answer. As the Services field CMFs in accordance with Joint Staff guidance, capability development should occur concurrently to ensure the CMF have the requisite facilities, platform, equipment, and tools needed to accomplish their assigned mission. In many cases, Cyber forces, to be operationally effective, would need to retain the capability to operate in a manner which conceals the detailed specifics of U.S. military capabilities. If we were to operate "in the clear," we may expose our tradecraft, tools, and infrastructure. If we do that, our enemy can deny us our capability and, in some cases, replicate it and use it against us.

Question. Section 932 of the NDAA for Fiscal Year 2014 requires the Secretary of Defense to provide CYBERCOM with infrastructure to enable CYBERCOM to independently access global networks to conduct military operations.

What are your views on this requirement?

Answer. There is no doubt that collocating CYBERCOM with NSA, and dual-hatting the Commander and Director, allows for efficient use of available platform capabilities and technical expertise. I do believe; however, that CYBERCOM needs additional infrastructure to accomplish military operations that are unique and distinguishable from the Intelligence Community. The Department has made significant progress recently in identifying and planning for development of alternative, diverse, scalable, deployable, and disposable platforms that can be available on demand to the CMF for mission accomplishment.

Question. What is your understanding of the Department's plan for complying with the legislation?

Answer. My understanding is that CYBERCOM has already been tasked by the Deputy Secretary of Defense and has made measurable progress in laying out a

strategy for identifying the numbers and mix of alternative platforms required to meet operational requirements, both for steady state and contingency purposes. These platforms will give the CMF the diversity and scalability needed to address the threat, apart from the intelligence platform. Additionally, since they do not require the breadth and sophistication of the existing platform, they should be less expensive to build and deploy.

Question. Do you believe DOD can implement the legislative direction in an effective and affordable manner?

Answer. Yes, there has been a significant amount of effort expended by the Department toward meeting this requirement.

DEVELOPMENT OF CYBER OFFICER CORPS

Question. In a forthcoming article, the J–3 of CYBERCOM, Major General Brett Williams, argues that: "We have a pressing need to develop cyberspace operators who are credible and effective in the J–3 and J–5, within both the Joint Staff (JS) and the combatant commands (CCMD). Just for emphasis, that is the J–3 and J–5, not just the J–2 and J–6; and at all of the CCMDs, not just CYBERCOM . . . Joint staffs consist of what we typically think of as operators, members of the combat arms who are educated, trained and experienced in operations. Cyberspace expertise usually comes from people with intelligence, communications or cryptology backgrounds; career fields typically categorized as support forces. If we are going to treat operations in cyberspace like operations in the other domains, the Services must commit to unique career fields for cyberspace . . . Cyberspace, like the other domains, requires officers who are developed across their careers in a way that positions them to lead at senior levels in both command and staff. Cyberspace officers should spend their first 10 years becoming tactically proficient in all aspects of cyberspace operations, complete service and joint military education, serve on joint staffs, command in their area of operational specialty and do all of the other things necessary to produce general and flag officers whose native domain is cyberspace."

What are your views about whether cyber officer career development should be distinct from both intelligence and communications officer development?

Answer. Specialized expertise in our officer ranks is critical to mission accomplishment. At the same time, a shared understanding across the team is essential. The way we have deliberately approached this in the Navy has been the establishment of Cyber Warrant Officers and Cyber Warfare Engineers. These individuals are purposefully selected to join our ranks from either our enlisted force, the Intelligence Community, academia, or industry. We then train and employ them to leverage their specialized expertise. They serve side by side with Officers from varied career fields, but primarily intelligence and communications specialists although combat arms officers could be trained as cyber officers as well. I believe all officers should have an appreciation for cyberspace operations. Intelligence and communication officers must have a clear understanding of the same, and we have a responsibility to develop specialized expertise in a core of cyber officers.

Question. Is it advisable to develop cyberspace officers as we do other combat arms or line officers? Why or why not?

Answer. I am a strong proponent of diversity across the team and quick to recognize all have a responsibility to both understand and contribute in this mission area. We must find a way to simultaneously ensure combat arms and line officers are better prepared to contribute, and cyberspace officers are able to enjoy a long, meaningful career with upward mobility. A meaningful career should allow them to fully develop as specialized experts, mentor those around them, and truly influence how we ought to train and fight in this mission space. I am especially interested in the merit of how a visible commitment to valuing cyberspace officers in our ranks will affect recruitment and retention. I believe that many of today's youth who are uniquely prepared to contribute (e.g. formally educated or self-developed technical expertise) do not feel there is a place for them in our uniformed services. We must find a way to strengthen the message of opportunity and I believe part of the answer is to do our part to ensure cyberspace officers are viewed as equals in the eyes of line and combat arms officers; not enablers, but equals. Equals with capabilities no less valued than those delivered by professional aviators, special operators, infantry, or surface warfare.

ALIGNMENT OF MILITARY CYBER OPERATIONS WITH CYBER INTELLIGENCE COLLECTION

Question. Do you think that, as CYBERCOM matures and as cyber military art develops, military cyber operations and cyber intelligence operations should be distinct operations?

Answer. Intelligence is a joint function integral to all military operations. Intelligence operations are conducted in cyberspace to inform military operations in all domains, including cyberspace.

Question. In the long term, what are the pros and cons of treating the Services' cyber organizations and the service cryptologic elements as distinct entities?

Answer. Just as there is a dynamic partnership between CYBERCOM and NSA, and the disciplines of military cyber operations and cyber intelligence operations are interwoven, there is a similar relationship and advantage to be had in the partnerships between the service cryptologic and cyber organizations. They provide key capability to their Services as independent focal points for warfighting and intelligence, but together provide the additive cyber capability for each Service. If confirmed, I will continue to assess the cyber force model as it develops in view of this synergism.

Question. Do you think that military cyber operations personnel assigned to CYBERCOM units should, in the long term, continue to be funded mainly in the intelligence budget and competing with intelligence priorities?

Answer. In view of our current fiscal environment and challenges, if confirmed, I would examine and assess all CYBERCOM funding streams and processes, including personnel.

RANGE SUPPORT FOR U.S. CYBER COMMAND

Question. Section 932 of the NDAA for Fiscal Year 2014 requires the Secretary of Defense to ensure that there are adequate range capabilities for training and exercising offensive cyber forces in operations that are very different from cyber intelligence operations.

What is your understanding of CYBERCOM's range requirements for individual and unit training, and exercises, and the capabilities and capacity of the joint cyber range infrastructure to satisfy those requirements?

Answer. It is my understanding that the persistent training and test environment is being developed based on requirements from CYBERCOM's exercise continuum of Cyber Knight, Cyber Guard, and Cyber Flag. This continuum is designed to train and/or certify CMF teams. Unfortunately, these exercises are executed using not only ad hoc range support, but also ad hoc facilities. Though the lack of a range continues to be a limiting factor, so does the lack of a physical infrastructure. Though the main effort in building the teams is individual training and qualification right now, collective training and certification will quickly make the lack of efficient range even more glaring than it is today. Our cyber forces need a persistent training environment they can depend on every day of the week to train. We must continually train against a high end adversary and not only in CJCS level exercises. The key to success here is training. A persistent range is a must have if we want to build a professional cyber force.

Question. What is your view of the NDAA legislation?

Answer. The Department continues to fully realize the potential of the DOD Enterprise Cyber Range Environment (DECRE) governance body to oversee Cyber Range issues. The main effort of DECRE is the establishment of a persistent test and training environment that will effectively meet the growing demand of the CMF teams. It is essential that we provide these teams, which are quickly reaching IOC and FOC in greater numbers, by providing on-demand environments for training in both offensive and defensive cyberspace operations. It is my understanding that the Department is on pace to deliver an assessment of the required cyber range capacity and capability to support CMF training by October 2014.

INFORMATION ASSURANCE

Question. The President's Review Group on Intelligence and Communications Technologies recommended that the Information Assurance Directorate (IAD) of the NSA be separated from NSA and subordinated to the cyber policy component of DOD. The Senate version of the NDAA for Fiscal Year 2014 included a provision that would transfer supervision of the IAD from the Under Secretary of Defense for Intelligence (USD(I)) to the Chief Information Officer (CIO). The committee's rationale for this transfer was that the IAD conducts cyber protection-related duties, which fall under the responsibility of the CIO, not the USD(I).

What do you see as the pros and cons of these proposals?

Answer. I support the President's decision for the IAD to remain part of NSA. NSA has developed (and continues to develop) an extremely deep cadre of computer scientists, mathematicians, software engineers, etc. whose skills are translatable across the breadth of the Information Assurance (IA) and SIGINT missions. IAD and the Signals Intelligence Directorate (SID) operate in a common trade space, the

global telecommunications network. NSA offensive and defensive missions have a proven track record of success at working together to counter the cyber threat. Code making and code breaking are two sides of the same coin. Breaking them apart will have significant consequences to the U.S. Government's ability to develop secure communications based on the understanding of how those communications might be attacked.

NSA has developed an infrastructure that supports both Information Assurance and SIGINT missions. Creating a separate agency that would need to develop and build its own infrastructure and expertise would be extremely inefficient and costly in a time of constrained resources. IAD guidance and technology helps secure the NSA enterprise. The work IAD performs benefits the security of the Nation and the world. Current Media Leaks have unfortunately caused degradation in our trust relationships with industry. If confirmed, I am committed to restore the trust and will deepen the partnerships with the DOD CIO and the USD(I) to demonstrate oversight procedures and processes function appropriately.

DUAL HATTING OF DIRECTOR OF THE NATIONAL SECURITY AGENCY AND THE COMMANDER, U.S. CYBER COMMAND

Question. The President's Review Group on Intelligence and Communications Technologies recommended that the positions of Director of NSA and the Commander of CYBERCOM be separated and that the President appoint a civilian to be Director of NSA. The President decided against separating these two positions at this time. According to press reports, the President based his decision, in part, on his perception that CYBERCOM was not yet mature enough to stand on its own without a very strong institutional connection to NSA.

If CYBERCOM remains too dependent on NSA for their leadership to be bifurcated, does it follow that CYBERCOM is not mature enough to become a full unified command?

Answer. My focus on sub-unified or unified will rest on what allows CYBERCOM to achieve the most effective cyber force—one that is best postured to defend the Nation and our national interests.

The decision by Secretary of Defense to redesignate the position of Director, NSA as both Commander, CYBERCOM and Director, NSA enabled DOD to leverage the similarities and overlaps between the capabilities needed for the conduct of NSA's core missions—SIGINT and IA—and those of CYBERCOM to provide for the defense and secure operation of DOD networks; and, upon order by appropriate authority, to operate in cyberspace to defend the Nation. The strength of this arrangement as the most effective approach to accomplishing both organizations' missions was re-affirmed with the President's December 2013 decision to retain the dual-hat position.

Question. To the extent that military operations in cyberspace should evolve to be different and distinct from intelligence collection in cyberspace, is it possible that NSA's strong influence over CYBERCOM's development could hinder, as well as support, the proper maturation of the Command? What are your views on this issue?

Answer. I will ensure NSA, as a combat support agency, continues to support CYBERCOM's ability to execute its mission as well as its maturation. For example, there is a high correlation between the knowledge, tools, and techniques necessary for meeting military objectives and those for enabling intelligence collection. This correlation allows economy of scale in tool and technique development. In addition, I will ensure that CYBERCOM has control over the assets it needs and I will work within DOD to ensure CYBERCOM has the support it needs to be successful. As the dual-hatted Director/Commander, I will empower the Deputy Director, NSA and Deputy Commander, CYBERCOM to focus on running their respective organization with mission equities in mind, while I maintain accountability with insight into both missions and direct collaboration when necessary.

Question. As NSA is a combat support defense agency subject to the authority, direction, and control of the Secretary of Defense, and NSA is subordinate to the Secretary of Defense in his capacity as the President's executive agent for SIGINT under Executive Order 12333, is there any reason to expect that NSA's support for CYBERCOM and the other combatant commands would be questionable if the dual-hat arrangement were ended?

Answer. NSA has a long history of supporting combatant commands with SIGINT and IA products and services, well before CYBERCOM was established. I will ensure NSA provides mission critical support to all combatant commands, with or without the dual-hat arrangement.

U.S. CYBER COMMAND AS A SUB-UNIFIED COMMAND

Question. The UCP establishes CYBERCOM as a sub-unified command reporting to STRATCOM. We understand that the administration considered modifying the UCP to establish CYBERCOM as a full combatant command.

What are the best arguments for and against taking such action now?

Answer. I understand that there was discussion at the CJCS and Service Chiefs' level in 2012 to establish CYBERCOM as a full unified command, and that discussion of this option has continued.

I don't believe there are any major impediments to elevating CYBERCOM to full unified command status, with the exception of adding approximately 112 personnel to our headquarters manning (currently 912) required to accomplish administrative functions that would accompany unified command status, such as workforce recruitment, Planning, Programming, Budgeting and Execution (PPBE); and Global Force Management. In addition, there are formal processes that would have to be executed, including revision to the current UCP language, but cyberspace operations comprise both a warfighting and enabling discipline and domain in and of itself. CYBERCOM is working incredibly hard every day to develop its forces, processes, and capability, so perhaps the best argument against elevating the command is the need to focus energies in these areas.

The argument for full unified command status is probably best stated in terms of the threat. Cyber attacks may occur with little warning, and more than likely will allow only minutes to seconds to mount a defensive action seeking to prevent or deflect potentially significant harm to U.S. critical infrastructure. Existing department processes and procedures for seeking authorities to act in response to such emergency actions are limited to unified combatant commanders. If confirmed, as the Commander of CYBERCOM, as a sub-unified combatant commander I would be required to coordinate and communicate through Commander, STRATCOM, to seek Secretary of Defense or even Presidential approval to defend the Nation in cyberspace. In a response cycle of seconds to minutes, this could come with a severe cost and could even obviate any meaningful action. As required in the current Standing Rules of Engagement, as a combatant commander, I would have the requisite authorities to directly engage with the Secretary of Defense or President of the United States as necessary to defend the Nation.

There are some inherent inefficiencies in not elevating, also, in the form of redundant processes and timeliness. Elevation to full unified status would improve resource advocacy, allocation and execution by improving input to Department processes and eliminating competition in prioritization. Additionally, alignment of responsibility, authority, situational awareness, and capability under a single commander would improve cyberspace operations and planning.

Question. What authorities for operating in cyberspace that are allocated to STRATCOM have been pre-delegated to CYBERCOM?

Answer. CYBERCOM has been delegated by Commander, STRATCOM, the responsibility to conduct specified cyberspace missions as detailed in section 18(d)(3) of the UCP. The specific missions delegated include: directing DODIN operations, securing and defending the DODIN; maintaining freedom of maneuver in cyberspace; executing full-spectrum military cyberspace operations; providing shared situational awareness of cyberspace operations, including indications and warning; integrating and synchronizing of cyberspace operations with combatant commands and other appropriate U.S. Government agencies tasked with defending the Nation's interests in cyberspace; provide support to civil authorities and international partners.

SUPPORT FOR THE COMBATANT COMMANDS

Question. The Secretary of Defense has ordered the Military Services and CYBERCOM to develop operational military cyber teams to support the missions of defending the Nation against cyber attacks, supporting the war plans of the geographic and functional combatant commands, and defending DOD networks against attacks. The mission teams that will support the combatant commanders ultimately will be under the operational control of those commanders. The committee understands that, to date, the combatant commands have not committed to creating cyber component commands to direct the operations of those units.

In your opinion, can the combatant commanders properly direct the operations of assigned cyber mission teams without a component command element?

Answer. Geographic combatant commanders already have the authority to direct and execute certain DCO within their own networks. These actions consist of DCO internal defensive measures (DCO–IDM) to prepare and protect mission critical networks. The current Joint Staff C2 model provides an interim construct to direct DCO–IDM through a Joint Cyber Center/Cyber Support Element. Combatant com-

manders direct full-spectrum Cyberspace operations (ISR, OPE, Attack and Defend) through a Joint Cyberspace Component Command to ensure actions are synchronized and integrated throughout all warfighting domains. A JFCCC also provides for accountability through legal oversight and compliance—a requirement for Cyberspace Operations. Until a JFCCC is established, a Joint Force Headquarters directly supports combatant command planning, execution, and oversight.

Question. Four years after the creation of CYBERCOM, to what extent have cyber operations been integrated into the operations plans of the combatant commands?

Answer. My understanding is that progress has been made in integrating cyberspace capabilities into the operations plans of the combatant commands. Although much work remains, CYBERCOM has been successful in this effort by coordinating and cooperating with the combatant commands directly, by integrating cyberspace capabilities when the plans are undergoing Department-wide review, and also by drafting cyberspace support plans that supplement the higher level combatant command plans.

Additionally, CYBERCOM is building 27 CMF teams assigned to the combatant commands to achieve exactly this kind of capability.

Question. How would you assess the progress of the Department in developing cyber capabilities for the use of the command cyber teams to support the specific needs of the combatant commands?

Answer. The Services have made progress developing capabilities to equip their CMF teams. At the Department's direction, CYBERCOM has established, and now chairs, the DOD Cyber Operational Capabilities Board (COCB) which will integrate military cyber capability development into existing requirements processes.

In accordance with Department direction, CYBERCOM has also begun implementing changes to the Cyber Capabilities Registry (CCR). The CCR is now populated and accessible, providing military planners a compendium of available cyberspace capabilities for use in support of mission requirements. Ultimately, the CCR will become an informative source for all DOD cyberspace capabilities.

CYBERCOM recognized that we needed to make progress faster in developing the tools our warfighters need in cyberspace. As such we stood up a J9 inside the command and staffed it with the best and most qualified military and NSA personnel (lead by a NSA senior and U.S. Army Colonel both with Ph.Ds) to work with the Services, industry, academia, the IC and our DOD labs to bring new ideas and tools to our cyber forces in the shortest time possible. This effort is starting to bear fruit delivering cyber tools our warfighters are already training with and integrating in tactical training exercise.

While the Department has made progress in this area, there is still much work to be done to ensure we develop joint, interoperable cyberspace capabilities to equip the CMFs as they become operational.

Question. What priority has been assigned to the development of capabilities for national versus command cyber mission teams?

Answer. The prioritization of capability development for national and combatant command CMFs flows directly from CYBERCOM's three mission areas: (1) defend the Nation; (2) secure, operate, and defend DOD information networks (DODIN); and (3) provide support to combatant commands. CYBERCOM's highest priority is to defend the Nation. This is done in parallel with activities dedicated to securing the DODIN and supporting combatant commands. We are building out a robust cyber force over the next 3 years. While we rightfully have first focused on the DTN mission, we have simultaneously begun the buildout and IOC of our Combatant Command CMTs and CPTs. All of these mission areas are resourced in a balanced way in accordance with a continuous threat assessment and fiscal limitations.

Question. Who would you say is responsible for developing cyber capabilities to support joint task forces and lower echelons?

Answer. The Services are responsible for developing capabilities to equip their forces. That said, CYBERCOM plays a role coordinating operational and technical requirements to ensure interoperability for CMFs and compatibility with mission infrastructures. The DOD Cyber Operational Capabilities Board (COCB) provides a venue for much of the coordination to standardize military cyber capability development and leverage existing programs to avoid duplication of effort across the DOD. In its unique position, CYBERCOM can and should form a community of operational and technical subject matter experts from across DOD and the IC to inform policy and resourcing decisions.

DEVELOPMENT OF CYBER CAPABILITIES

Question. CYBERCOM has depended heavily to date on NSA for technology, equipment, capabilities, concepts of operations, and tactics, techniques, and procedures.

Are you satisfied that DOD is organized and resourced to provide a broad base of innovation and capability development in the cyber domain that includes the Military Service's research and development organizations, Defense agencies such as the Defense Advanced Research Projects Agency, and the private sector?

Answer. While the Department has made much progress, more work certainly remains to ensure that DOD is organized and resourced to provide military-specific cyber capabilities. However, I believe the Department is moving in the right direction through a series of decisions to prevent redundancy and to ensure cyber innovation in both the public and private sectors can be leveraged. One of these decisions was to establish the aforementioned COCB to identify and track dependencies among capability requirements and to validate and prioritize all cyberspace capability requirements.

CYBERCOM's Advanced Capabilities Directorate, J–9 has existing relationships with the Services and their dedicated research and development labs, DARPA, federally-funded research and development centers, the defense industrial base, the private sector, and other entities, allowing CYBERCOM to leverage their expertise to provide and build diverse capability to enable full-spectrum military operations. As a member of the COCB, the J–9 also helps enforce a process to ensure there is no redundancy of effort, and that several DOD entities can use the same capability multiple times when possible to get more return on investment.

DELEGATION OF SIGNALS INTELLIGENCE AUTHORITIES

Question. How important will it be for CYBERCOM personnel to be able to operate with SIGINT authorities that are not necessarily tied to NSA personnel who may be working temporarily for CYBERCOM?

Answer. The ability of CYBERCOM personnel to operate under delegated SIGINT authorities and leverage the national cryptologic platform is a critical capability, enabling the command to fully execute its cyberspace mission in an informed, timely, and coordinated manner. SIGINT information remains vital to support cyber operations. Effective "net-speed" operations as conducted by an expanded U.S. CMF require ready access to the technical streams of information that SIGINT provides. Providing SIGINT information at the lowest possible level in a distributed force environment makes the delegation effort especially important. Time delay increases the potential for mission failure. It is important to note that under delegated SIGINT authorities, CYBERCOM personnel adhere to the same uniform techniques, training and standards, as well as intelligence oversight and compliance programs, as those who work for the NSA. We will not sacrifice our legal and security obligations to accomplish these goals.

JOINT INFORMATION ENVIRONMENT

Question. The DISA advertises the Joint Information Environment (JIE) programs as delivering:

> "... the largest restructuring of information technology (IT) management in the history of the DOD. The end state is a secure, joint information environment comprised of shared IT infrastructure, enterprise services, and a single security architecture. JIE will enable DOD to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies."

To realize this potential, the CYBERCOM will have to operate within the JIE.

Has CYBERCOM developed plans for integrating its warfighting operations into the JIE?

Answer. In the JIE Management Construct (approved at the TANK), CYBERCOM is responsible for identifying requirements and concepts of operation which enable and align with the Command and Control (C2) and defense of the DODIN. JIE is a framework for which standards are being designed and built to meet these specified operational requirements.

Question. Will the JIE systems architecture support a full range of potential CYBERCOM warfighting operations?

Answer. The JIE systems architecture supports the full range of operations 'of' and 'on' the DODIN. The JIE will shift focus from protection of Military Service-specific networks, systems, and applications to securing data and its uses; a paradigm shift from the traditional net-centric to a data-centric environment. Key secu-

rity features that will be employed under the JIE framework include: an enterprise-wide Single Security Architecture (SSA), a secure Out-of-Band Management network; standardized identity and access management; and the integration of thin-client and cloud-based (virtualization) technologies.

JIE changes the way the Department delivers IT capabilities in the largest, most complex operational environment in the world. Common services and capability will provide users information at the point of need from any networked device and from the enterprise level for all users. The ultimate beneficiary of the JIE will be the commander in the field and forces at the tactical edge. JIE will allow better integration of information technologies, operations, and cyber security at a tempo that supports today's fast-paced operational conditions. The operational capabilities delivered through the JIE will enable commanders to blend the art of command with the science of control, enabling JF 2020 to address emerging military challenges through the flexible integration of warfighting functions as required.

JIE will afford organizations responsible for operating and defending this complex environment end-to-end visibility and situational awareness for security from strategic to tactical as well as down to the desktop. It will eliminate the barriers which prevent information sharing and consolidate computing power and storage capabilities while enabling support for low-bandwidth/disadvantaged users.

Question. Should DOD approach the JIE as more of a "weapons system" than a pure IT system in order to support the range of CYBERCOM's warfighting plans?

Answer. JIE is not a system, but is a framework of standards which the DOD Services and Agencies are using to procure, operate, and defend the DODIN. JIE is focused on helping the DOD achieve full spectrum superiority, improved mission operational effectiveness and increased security while realizing IT efficiencies. The JIE focuses on creation of a secured joint environment, comprised of a shared Information Technology infrastructure that will deliver common services from the enterprise, bound and secured by a single security architecture. The environment will be operated in accordance with responsibilities and authorities identified in the UCP based on common, enforceable standards and specifications, as well as common tactics, techniques, and procedures. The primary objective of creating the JIE is to provide DOD and mission partners secure access to Department IT capabilities at the point of need; i.e., home, work or deployed; by creating a Joint Enterprise Information Environment that encapsulates computing power; common enterprise services and mission applications; and access to data anywhere in the enterprise with the ability to extend the same capabilities in the deployed environment. However, once we build the underlying architecture(s) within the JIE framework, we need to look at them as a weapons system: measure its readiness, garner mission assurance, produce trained and ready operators, et cetera.

SECURITY OF NAVY NETWORKS

Question. The Wall Street Journal last September reported that Iran had compromised the Navy Marine Corps Intranet (NMCI), an unclassified but important and pervasive internal communications network. The Navy has made an award for the successor to NMCI, called the Next Generation Enterprise Network (NGEN). The winning contractor is the same company that bought the original contractor for NMCI.

Is the NMCI properly architected and constructed against external cyber attacks? If not, why not?

Answer. Yes, NMCI is properly architected and constructed against external cyber attacks. Since its inception the NMCI architecture has evolved to respond to the threat environment. The threat environment has clearly changed and cyber security improvements have been made to NMCI over the years. The Navy and DOD defense in depth cyber security architecture, when combined with NMCI security layers, provide appropriate protection. As with all networks, the NMCI security architecture continues to mature as technology and threats evolve. Based upon operations over the last 8 months and in collaboration with NSA, USCC, and DISA, I have identified additional network hardening and cyber security requirements for current and future Navy Networks that are currently being planned and programmed for implementation.

Question. Is the NGEN architecture more secure than NMCI, and if so, in what respects?

Answer. Yes, NGEN benefits from lessons learned and technological advances but is designed on the same solid security principles used to develop NMCI. Its increased security will be the byproduct of three important factors: increased Navy Command and Control (C2) of a network the Navy "bought back" as a result of the transition from a contractor-owned/contractor-operated model to a government-

owned/contractor-operated model; an increase in the Navy's ability to make and implement critical decisions about the selection of enterprise services under a more agile and innovative contract; and a firm commitment to align those services with the higher level JIE and Intelligence Community (IC) Information Technology Enterprise. The NGEN contract also allows us to add, modify, and delete services in addition to lowering overall operating costs through competition.

Question. Is the NGEN program fully aligned with the security architecture of the JIE initiative? If not, why not?

Answer. Yes, NGEN is designed and architected to current security standards and will leverage Technical Refresh and additional security funding to align to the JIE SSA as it becomes better defined, documented, and tested. Navy is participating actively in DOD's drive to define the SSA and the other components that will come together to form JIE. It has been playing a particularly active and important role in defining how the emerging SSA and related components will apply to JIE Increment II, which will properly secure U.S. and multinational information flows under the transformational Mission Partner Environment. As the definitions take shape, Navy will take decisive action to bring NGEN into alignment with JIE's SSA.

Question. What steps and how much time and investment will it take to align NGEN with JIE?

Answer. The Navy supports the concept of JIE and is working in coordination with the other Services, DISA, COCOMs, and OSD to fully develop this concept into a joint enterprise capability. By continuing such engagement, Navy will develop better insights regarding the time and money required to bring its NGEN into alignment with these higher-level architectures. At present, we are of the belief that our agile and innovative contracts and the investments we've already programmed across the Future Years Defense Program within NGEN and our other IT infrastructure and network programs (e.g., Consolidated Afloat Networks and Enterprise Services (CANES) and OCONUS Navy Enterprise Network (ONE–Net)) constitutes a sufficient response to the challenge at hand. As the standards for JIE mature, Navy will be able to provide cost and schedule estimates using NGEN as our path to meet JIE standards.

CYBER PERSONNEL

Question. What is your understanding of the direction DOD has given to the Military Services regarding the quality and existing skill levels of the personnel they will provide for the CMFs?

Answer. On behalf of the DOD (IAW CJCSI 3500.01G), CYBERCOM establishes CMFs joint standards for individual and collective training. These standards are contained in three foundational documents; the Joint Cyberspace Training and Certification Standard (JCT&CS), the Individual Training Pipelines, and the Training and Readiness Manual (T&R Manual). The JCT&CS identifies the unique Knowledge Skills and Abilities (KSAs) for each work role on the CMF Teams. The individual training pipelines outline an optimal path to achieving the required KSAs to satisfy the JCT&CS requirements. The T&R Manual provides the tasks, conditions and standards required to demonstrate individual and collective proficiency.

Question. So far, does it appear that there is a satisfactory match between the skills and aptitudes of the personnel provided by the Services and the training programs developed by CYBERCOM?

Answer. The CMF build out, when complete, will include over 6,100 personnel organized across 133 teams in the CMFs. As we build this force, work roles have unique training requirements and we must continue to create sustainable, repeatable training programs to meet this demand. Over the past 18 months, we've come a long way working out training pipeline bottlenecks. Additionally, over the next 2½ years of the CMF build, the Services must continue for the Services to incorporate CYBERCOM training requirements into their training programs, and ensure their workforce meets the CMF standards.

If confirmed, one of my first priorities will be to work closely with NSA and the Services to expand existing training classes, identify training equivalencies, and establish alternate training venues. I think we should also look collectively at increasing the time on station requirements to retain trained and fully qualified personnel until sufficient training programs are in place.

Question. What direction has been given to the Services regarding recruiting goals and priorities for individuals with skills and aptitudes relevant to the needs of CYBERCOM?

Answer. Senior DOD leadership directed the Services to establish management processes that identify, recruit, retain and provide incentivized career advancement paths for military and civilian personnel. This allows the high-end advanced skills

that CYBERCOM has identified to work in the CMF. Progress is being made by each Service and the issue is monitored closely in monthly reporting by CYBERCOM to the Joint Staff. DOD is addressing one of the more significant challenges by looking at options pertaining to the civilian workforce that would establish a flexible and responsive workforce that improves the ability to attract, develop, motivate and retain a high quality Cyber workforce.

Question. Has the Department considered delegating personnel authorities to CYBERCOM that are similar to those that are exercised by U.S. Special Operations Command to ensure that the Services manage the careers of their servicemembers with cyber skills appropriately?

Answer. SOCOM's Article 167 Authorities continue to prove essential to their ability to work with the Services to develop truly Joint capabilities that meet Joint Standards. CYBERCOM continues to do a great job facilitating progress without such authority, but eventually delegating these authorities could greatly enhance their ability to meet the Nation's needs.

Question. What would be the pros and cons of providing CYBERCOM such authorities?

Answer. While there are no real cons in my opinion, the pro for CYBERCOM is the same as for SOCOM. This authority would allow CYBERCOM to shape the cyber force and ensure cyber training and capabilities are standardized and inherently Joint across the man, train, and equip spectrum. Once trained, these personnel are highly skilled and valuable commodities. They are bona fide high-demand, low-density assets—just as our Special Operations Forces are.

We are growing a highly-skilled, highly-qualified standardized workforce.

CYBERCOM, empowered with these types of authorities can more effectively advocate and ensure that we do everything in our power to retain these exceptional forces even as our manpower, promotion, and retention systems may be slow to recognize this.

DESIGNING THE INTERNET FOR BETTER SECURITY

Question. How could the Internet be redesigned to provide greater inherent security?

Answer. Advancements in technology continually change the architecture of the Internet. Cloud computing, for instance, is a significant change in how industry and individuals use Internet services. As evidenced by the growth of security conferences, companies and media attention, security is at the forefront of Internet use as businesses and government strive to protect intellectual property and citizens desire to protect their privacy. To put it simply, the environment is ripe for significant attention to inherent security and government, industry, and academia all have an interest in achieving this objective.

I believe there are options for the Internet to provide greater inherent security. Several major providers of Internet services are already implementing increased security in email and purchasing services by using encryption for all transmissions from the client to the server. It is possible that the service providers could be given more responsibility to protect end clients connected directly to their infrastructures. They are in a position to stop attacks targeted at consumers and recognize when consumer devices on their networks have been subverted. The inability of end users to verify the originator of an email and for hackers to forge email addresses have resulted in serious compromises of end user systems. If confirmed, I look forward to working with this committee, as well as industry, academia and government leaders, on the advancement of security measures for the Internet.

Question. Is it practical to consider adopting those modifications?

Answer. I believe modifications to enhance security on the Internet will evolve and strengthen over time. Industry is developing and deploying solutions today to maintain the trust of their clients. Events such as recent payment card breaches are highlighting the concerns and accelerating solution deployment. These advancements in commercial technologies provide a benefit to all who use them, including government. Public-private working groups have and will continue to address hard problems and implementable solutions to strengthen security on the Internet.

Question. What would the impact be on privacy, both pro and con?

Answer. I believe the Government should strive to implement advanced security measures that enhance privacy. Tensions between security and privacy are not new, but I believe we cannot accept one without the other. Increased security should help protect identities, reduce cyber attacks, and assure the transmission and storage of private data; in turn, this enhanced security will ultimately improve individual and corporate privacy in the Internet. If confirmed, I look forward to working with this

committee and industry and Government leaders to protect privacy while making the Internet as secure as possible.

THE SECTION 215 PROGRAM

Question. In January, 2014, the President ordered a transition to end the section 215 telephone metadata collection program as it currently exists, to "preserve the capabilities we need" without the government collecting and holding the data on call detail records.

What are your views on what specific capabilities need to be preserved as the program is transitioned?

Answer. The program grew out of a desire to address a gap identified after September 11. One of the September 11 hijackers—Khalid al-Mihdhar—made a phone call from San Diego to a known al Qaeda safe-house in Yemen. NSA saw that call, but it could not see that the call was coming from an individual already in the United States. The telephone metadata program under section 215 was designed to map the communications of terrorists so we can see who they may be in contact with as quickly as possible. It does not involve the content of phone calls or the names of the people making the calls.

I believe that we need to maintain an ability to make queries of phone records in a way that is agile and provides results in a timely fashion. Being able to quickly review phone connections associated with terrorists to assess whether a network exists is critical.

Question. From your perspective, what are the pros and cons, and problems, involved in the establishment or designation of a private "third party" to hold the data, on the one hand, and the service providers keeping the data, on the other?

Answer. Both options are technically feasible and, if implemented in a manner that addresses mission requirements, could be viable alternatives for the current program. I anticipate that either would require significant upfront costs. However, if a private "third party" holds the data, I expect it would be at greater expense and could introduce other complexities. For example, as the President noted in his speech on 17 January 2014, it could require companies to alter their procedures in ways that raise new privacy concerns. If the service providers keep the data, I understand that this may require statutory changes for any data retention requirements which may be levied upon them.

Question. What is your assessment of the impact on the program of the President's order to have the Foreign Intelligence Surveillance Act (FISA) Court make individual Reasonable, Articulable Suspicion (RAS) determinations prior to non-emergency database queries?

Answer. Before the President's speech on January 17, 2014, this approval process was done internally at NSA and both DOJ and ODNI conducted post-approval reviews of RAS determinations on a quarterly basis. Since 17 January, NSA has been working closely with DOJ to establish processes and procedures to obtain RAS approvals from the FISA court.

Question. The Federal Communications Commission requires service providers to keep telephone call detail records for 18 months. The government currently keeps the records collected under section 215 for 5 years. Section 215 expires next year. If Congress does not renew the provision, the executive branch could continue to access call records under other authorities, but only through the service provider's repositories.

Is that a viable alternative?

Answer. The other authorities, as currently established, do not fully replicate the current ability under section 215 to obtain telephony metadata records in a way that is agile and timely. However, I believe it's possible that, if new legal authorities were established or existing authorities were modified to enable more flexible acquisition of such records, these could serve as a viable alternative.

Question. How critical is it in your opinion to have guaranteed access to records more than 18 months old from all service providers?

Answer. Currently, NSA retains the metadata for 5 years, but it is my understanding that NSA has assessed that the 5-year retention period could be reduced to a shorter period without significantly decreasing operational utility. In his January speech, the President directed a study of how to restructure the program for the longer term. The work of that study, with participants from multiple agencies, is now ongoing. While specific options are under development, there is further work to be done.

Question. What concerns do you have, if any, about leaving the metadata records with the service providers, and having them produce records responsive to Court-approved queries?

Answer. My main concern is whether such an arrangement would produce records in a timely fashion. Being able to quickly review phone connections associated with terrorists to assess whether a network exists is critical. The ongoing interagency review is looking at ways to address this risk.

SECTION 215 UTILITY VERSUS PRIVACY CONCERNS

Question. The Privacy and Civil Liberties Oversight Board (PCLOB) and the President's Review Group On Intelligence and Communications Technologies ("Review Group") characterized the section 215 program as useful but not critical. The PCLOB stated that "We have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation."

What is your understanding of the utility of the program, and how that utility compares to the level of concern among the American people about its perceived impact on privacy and civil liberties?

Answer. One of the key vulnerabilities identified after September 11 was the lack of a sufficient and timely capacity to detect when a known foreign based terrorist threat was in contact with someone inside the homeland. The section 215 program was designed to provide that capability by enabling the government to quickly review telephone connections to assess whether a terrorist network exists and the President has stated that it is critical the capability that this program was designed to meet is preserved. The President has also been clear about expectations that such a capability be conducted in a manner that addresses the concerns of the American people about the potential impact on privacy and civil liberties. I support the ongoing interagency effort in response to the President's direction to seek to find an ability for this necessary capability to exist within an acceptable privacy and civil liberties regime.

Question. The Review Group also stated on multiple occasions that the 215 program, contrary to many public reports, actually only collects "a small percentage of the total telephony metadata held by service providers."

How do the costs compare for expanding the government's capacity to ingest all telephony call records, on the one hand, versus the cost of enabling comprehensive access to needed records through the service providers, on the other?

Answer. In the summer and fall of 2013, NSA performed some analysis of the relative costs of having the Government collect the data in bulk with the costs of searching data retained at the providers. I have not been briefed on the details or the results of that analysis, or how it might apply to specific proposals now under consideration. If I am confirmed for this position, it will be my responsibility to thoroughly and accurately communicate costs and benefits to those who set policy and establish appropriations. Cost will be a factor taken into consideration in the development of options for the President. If confirmed, I will ensure that Congress will be informed of the cost of any successor programs.

REFORM OF THE FISA COURT

Question. The President's Signals Intelligence Directive (PPD–28) announced in January called for Congress to authorize a panel of advocates from outside the government to "provide an independent voice in significant cases" before the FISA Court. A similar approach has been recommended by the PCLOB and the President's Review Group.

Do you have any concerns about introducing an adversarial element in the proceedings of the FISA Court as the President and others have urged?

Answer. I concur with the President's view that responsible actions which will help increase the transparency of and confidence in the government's conduct of extraordinary authorities—like those performed under statutory authority with the Foreign Intelligence Surveillance Court—are an important element of government's relationship with the American people. If the legislative and judicial branches of government introduce changes to the FISA court or its proceedings, and if I am confirmed, I will be fully prepared to work with them and alongside others in the executive branch. Whatever approach is considered, I believe must also address the necessary timeliness and operational integrity of national security activities.

STANDARDS FOR SEARCHING NSA DATABASES USING U.S. PERSONS' PERSONALLY IDENTIFIABLE INFORMATION

Question. NSA collects foreign intelligence information under multiple authorities, including Executive Order 12333, traditional individualized FISA Court orders, and programs such as section 702 of the FISA Amendments Act, and section 215 of the Patriot Act. Unlike EO 12333 collection, traditional FISA wiretaps must meet a

probable cause standard and are very specifically targeted. The section 215 program involves bulk collection, but only of non-content metadata, and the bulk data is queried under the RAS standard that the target of the query is associated with terrorist groups. Section 702 content collection is based on the "reasonable belief" standard that the specific target of the collection is a non-U.S. person located outside the United States. The President's Review Group On Intelligence and Communications Technologies ("Review Group") and the PCLOB have raised issues about the standards under which the government can search through data holdings acquired under these authorities using U.S. persons identifiers.

Is NSA permitted to search data acquired under EO 12333 authorities using U.S. persons identifiers without probable cause?

Answer. Minimization procedures that are reasonably designed to protect the privacy interests of United States persons. The full procedures are classified, but generally prohibit selection of the content of communications of or concerning a U.S. person absent probable cause. However, there are exceptions, such as when there is a threat to life or when the search is limited to querying information under which there is no reasonable expectation of privacy (e.g. metadata).

Question. If so, what is your understanding of the legal justification? Does the review group's recommendation, relate to or cover queries of data acquired under EO 12333?

Answer. I defer to the Department of Justice (DOJ) for any legal interpretation of the procedures approved by the Attorney General.

Question. Is NSA allowed to search data acquired under traditional FISA individual wiretap orders using U.S. persons identifiers without probable cause?

Answer. Information acquired by NSA under traditional FISA orders must be handled in accordance with the Court-approved minimization procedures, as defined by FISA, that are reasonably designed to protect the privacy interests of U.S. persons. NSA's Court-approved minimization procedures for traditional FISA orders do not permit data searches using U.S. person names or identifiers. Any exceptions to these procedures would require approval by the Federal Intelligence Surveillance Court (FISC).

Question. If so, what is your understanding of the legal rationale?

Answer. I defer to the DOJ for any legal interpretation of the procedures approved by the FISC for individual FISA wiretap orders.

Question. What is your understanding of the legal rationale for NSA to search through data acquired under section 702 using U.S. persons identifiers without probable cause?

Answer. Information acquired by NSA under section 702 of FISA must be handled in strict accordance with minimization procedures adopted by the Attorney General and approved by the Foreign Intelligence Surveillance Court. As required by the statute and certifications approving Section 702 acquisitions, such activities must be limited to targeting non-U.S. persons reasonably believed to be located outside the United States. NSA's Court-approved procedures only permit searches of this lawfully acquired data using U.S. person identifiers for valid foreign intelligence purposes and under the oversight of the DOJ and Office of Director of National Intelligence.

Question. What is your understanding of the legal rationale for searching through the "Corporate Store" of metadata acquired under section 215 using U.S. persons identifiers for foreign intelligence purposes?

The section 215 program is specifically authorized by orders issued by the Foreign Intelligence Surveillance Court pursuant to relevant statutory requirements. (Note: the legality of the program has been reviewed and approved by more than a dozen FISC judges on over 35 occasions since 2006.) As further required by statute, the program is also governed by minimization procedures adopted by the Attorney General and approved by the FISC. Those orders, and the accompanying minimization procedures, require that searches of data under the program may only be performed when there is a Reasonable Articulable Suspicion that the identifier to be queried is associated with a terrorist organization specified in the Court's order.

INFORMATION SHARING LEGISLATION FOR CYBERSECURITY

Question. Several proposed cybersecurity bills have been introduced to authorize the collection and sharing of information on cybersecurity threats—including malware, command and control, exfiltration of data, and other evidence of compromise—between the public and private sectors for the purpose of enabling the private sector and Government to defend themselves, enabling law enforcement agencies to detect criminal activities and identify and prosecute perpetrators, and, in the

case of nation-states, enabling the Government to attribute attacks and hold aggressors accountable. To date, none of these proposals have been enacted.

In your view, would it be helpful for Congress to enact more limited legislation to enable the private sector to collect and share cyber threat information within the private sector, leaving the issue of sharing with the Government for the future?

Answer. The nature of malicious cyber activity against our Nation's networks has become a matter of such concern that legislation to enable real-time cyber threat information sharing is vital to protecting our national and economic security. Incremental steps such as legislation that addresses only private sector sharing would have limited effectiveness, because no single public or private entity has all the necessary authorities, resources, or capabilities to respond to or prevent a serious cyber attack. Therefore, we must find a way to share the unique insights held by both government and the private sector. At the same time, legislation must help construct a trust-based community where two-way, real-time sharing of cyber threat information is done consistent with protections of U.S. person privacy and civil liberties.

Question. What restrictions would you recommend be imposed on what information could be shared with the Government regarding cyber threats, and the uses to which the Government could apply that information?

Answer. Protecting the security and the privacy of Americans is not a mutually exclusive proposition. The information provided to the Government should be limited to that which is necessary for the Government to understand or take action to counter a cyber threat and to which all appropriate mechanisms have been applied to protect the privacy and civil liberties of U.S. persons. If confirmed, I would expect to engage fully in discussions on how to accomplish these objectives.

Question. What transparency measures and institutional checks would you recommend to increase confidence that allowing the sharing of cyber threat information would not lead to abuses of privacy and civil liberties?

Answer. Transparency can be ensured by establishing procedures for receiving, retaining, using, and disclosing cyber threat information. In turn, compliance with these procedures should be subject to independent review and oversight by cleared trusted U.S. Government and private sector third parties. Due to the criticality of real-time sharing of cyber threat information, we must also leverage technology that enables a transparent, policy-based, machine-speed infrastructure that automatically enforces the rules for use and any lawful restrictions on sharing.

CONGRESSIONAL OVERSIGHT

Question. In order to exercise its legislative and oversight responsibilities, it is important that this committee and other appropriate committees of Congress are able to receive testimony, briefings, and other communications of information.

Do you agree, if confirmed for this high position, to appear before this committee and other appropriate committees of Congress?

Answer. Yes.

Question. Do you agree, when asked, to give your personal views, even if those views differ from the administration in power?

Answer. Yes.

Question. Do you agree, if confirmed, to appear before this committee, or designated members of this committee, and provide information, subject to appropriate and necessary security protection, with respect to your responsibilities as Commander, CYBERCOM?

Answer. Yes.

Question. Do you agree to ensure that testimony, briefings and other communications of information are provided to this committee and its staff and other appropriate committees?

Answer. Yes.

Question. Do you agree to provide documents, including copies of electronic forms of communication, in a timely manner when requested by a duly constituted committee, or to consult with the committee regarding the basis for any good faith delay or denial in providing such documents?

Answer. Yes.

[Questions for the record with answers supplied follow:]

QUESTION SUBMITTED BY SENATOR JOE MANCHIN III

WHISTLEBLOWER PROTECTION

1. Senator MANCHIN. Vice Admiral Rogers, the disclosure of classified and sensitive information by Edward Snowden certainly highlighted serious flaws in the National Security Agency's (NSA) internal security. There are those that would call Snowden a whistleblower, but I am curious as to whether he made an attempt to address his concerns through existing whistleblower channels in the NSA. What were those channels at that time and how have they changed since?

Admiral ROGERS. The Intelligence Community Whistleblower Protection Act (ICWPA) and Presidential Policy Directive-19 (PPD–19) describe specific steps to be taken to file a complaint. It provides employees and contractors of intelligence agencies with a mechanism for reporting alleged wrongdoing in IC agencies and associated programs to Congress. Congress specifically extended whistleblower protection to contractors in 2009 and those protections remain in place today. Mr. Snowden did not follow the processes established by the ICWPA or PPD–19 and therefore is not a "whistleblower" as that term is defined.

In the case of Mr. Snowden, he had the option reporting through his chain of command or contacting any Inspector General. There are also Congressional committees and mechanisms in place. After extensive investigation, we have not found any evidence to support Mr. Snowden's contention that he brought these matters to the attention of anyone.

QUESTIONS SUBMITTED BY SENATOR KIRSTEN E. GILLIBRAND

RECRUITING TALENT IN U.S. CYBER COMMAND

2. Senator GILLIBRAND. Vice Admiral Rogers, the National Commission on the Structure of the Air Force recently released their findings, which highlighted the importance of the National Guard and Reserve in the U.S. cyber mission. Specifically, it noted that the Guard and Reserve were uniquely positioned, because of their part-time status, to attract and retain the best and the brightest in the cyber field. Additionally, the National Defense Authorization Act (NDAA) for Fiscal Year 2014 has directed the Department of Defense (DOD) to look at the integration of the Guard in all its statuses into the cyber workforce. I have long agreed with this assessment, and introduced the Cyber Warrior Act which would establish National Guard cyber teams in each State to leverage this talent pool. If confirmed, what is your vision for the roles of both the Guard and Reserve in U.S. Cyber Command (CYBERCOM) and within the distinct Service cyber elements?

Admiral ROGERS. CYBERCOM envisions the Guard and Reserve will play a vital role in our cyber mission by working through the Services for the opportunity to leverage their civilian skill sets, the dual mission of the Guard, and the complementary nature of reservists to address specific needs, fill gaps and provide a surge capability within the Active component.

3. Senator GILLIBRAND. Vice Admiral Rogers, I want to be helpful to DOD in recruiting the best talent and acquiring the best tools for our cyber mission. In your opinion, what can Congress do to assist DOD in this effort?

Admiral ROGERS. The Cyber Mission Force (CMF) construct and the corresponding planning documentation, identifies the size and scope of the CMF, the associated knowledge, skills, and abilities required for the various work roles that make up the CMF, the schedule for manning the teams, and the work role priorities. Together this information provides the Services with their targeted recruiting goals and priorities.

4. Senator GILLIBRAND. Vice Admiral Rogers, what do you believe DOD needs in order to remain on the cutting edge of cyber defense?

Admiral ROGERS. DOD requires trained and ready cyber teams that can take a more proactive approach rather than the reactive approach. DOD also requires a more defensible, data-centric architecture with cloud-enabled analytics, and a dynamic and reconfigurable network. CYBERCOM requires appropriate authorities to defend U.S. national interests in cyberspace. Additionally, policy is required that clearly establishes roles and responsibilities across agencies that provide the authority to see and defend systems outside of the DOD Information Systems.

CYBER DEFENSE

5. Senator GILLIBRAND. Vice Admiral Rogers, you are nominated to serve as both Commander, CYBERCOM, and Director, NSA/Chief, Central Security Service, giving you a unique role and perspective on cyber issues. What do you think are DOD's two most important cyber needs for the next 5 years?

Admiral ROGERS. Recently, General Alexander described to the House Armed Services Committee five key things we need to do without further delay, namely: promote a defensible architecture; develop a trained and ready workforce; pass cyber legislation that enables two-way, real-time information sharing among and between private and public entities; set up a seamless cyber command and control structure from the President on down; and, build a common picture to strengthen our Nation's cybersecurity defenses.

6. Senator GILLIBRAND. Vice Admiral Rogers, if confirmed, how will you incorporate cyber forces, especially in the National Guard, into our Homeland defense strategy?

Admiral ROGERS. The CYBERCOM Guard Reserve office is diligently working with the National Guard Bureau and U.S. Northern Command to develop a cyberspace strategy framework that incorporates relevant portions of our Homeland defense strategy involving the protection of our Nation's critical infrastructure and key resources.

7. Senator GILLIBRAND. Vice Admiral Rogers, what are your thoughts on the relationship between the Department of Homeland Security (DHS) and DOD in terms of global cybersecurity roles and responsibilities?

Admiral ROGERS. Global cooperation on cybersecurity is necessary to address the threat, build consensus on the norms of responsible conduct in cyberspace, and address ongoing malicious activity. CYBERCOM strongly endorses the U.S. Government's team approach, leveraging all of our homeland security, law enforcement, and military authorities and capabilities, which respectively provide for domestic preparedness, criminal deterrence and investigation, and national defense. As such, Department of Justice (DOJ), DHS, and DOD each have specific, critical roles and responsibilities as part of the Federal whole-of-government effort to counter cyber threats. Moreover, all three departments are involved with private and international partners within their areas of responsibility, and whether their activities are at home or abroad, the departments support one another to address cyber issues. As with threats to the United States, our allies, and our interests in other domains, DOD has the mission to defend the Nation, to include the protection of national security systems. This responsibility logically extends to all domains, including cyberspace. DHS is responsible for securing unclassified Federal civilian Government networks and working with owners and operators of critical infrastructure to secure their networks through risk assessment, mitigation, and incident response capabilities. DOJ is the lead Federal department responsible for the investigation, attribution, disruption, and, and as appropriate, prosecution of cybersecurity incidents. As authorized by the President, and consistent with the law, DOD defends, deters, and takes decisive action in cyberspace to defend national interests; supports DHS in homeland security (i.e., personnel, equipment, and facilities); and supports Federal agencies pursuant to the Defense Support of Civil Authorities process.

8. Senator GILLIBRAND. Vice Admiral Rogers, the dynamic nature of the cyber threat presents a unique problem in that we typically find ourselves in a perpetual game of catch-up, always chasing our adversary. As soon as one system fix is introduced, countless other vulnerabilities, some known, many unknown, become all the more magnified. If confirmed, how do you intend to address the continually morphing requirements distinct to the cyber threat facing both DOD and the United States as a whole?

Admiral ROGERS. [Deleted.]

9. Senator GILLIBRAND. Vice Admiral Rogers, what do you project as the main over-the-horizon cyber threat?

Admiral ROGERS. [Deleted.]

CYBER TRAINING

10. Senator GILLIBRAND. Vice Admiral Rogers, I am interested in the training our cyber warriors are receiving. What is your understanding of the training capacity at the Service academies and in the current pipeline?

Admiral ROGERS. Each Service Academy educates our future Service and joint leaders slightly differently and for good reason. The mission of the Service Academies is to educate our next generation of military leaders and cyber related skills are core to every officer regardless of their chosen career. Given the many requirements levied upon midshipmen and cadets, I believe the investment currently being made in cyber education to be appropriate.

11. Senator GILLIBRAND. Vice Admiral Rogers, do you see room for improvement in the training pipeline and at the Service Academies?

Admiral ROGERS. There is always room for improvement, and each Service Academy is integrating cyber education to meet Service specific needs. Because I am a Naval Officer, I am far more aware of how the Naval Academy has embraced cyber related education. 100 percent of their graduates will receive at least two semesters of technical cyber education with a large percentage of them earning a STEM degree. I believe that is the right path and one that each academy should consider implementing.

12. Senator GILLIBRAND. Vice Admiral Rogers, is there a role for Congress to assist in making improvements, such as a need for additional authorities?

Admiral ROGERS. Providing CYBERCOM with the oversight authorities it needs to ensure that it can enforce common, joint architectural components to support both CYBERCOM strategic requirements and unique Service specific requirements remains critical. I am still investigating the need for additional authorities and won't hesitate to make requests known if we deem them to be necessary.

RETENTION OF CYBER PERSONNEL

13. Senator GILLIBRAND. Vice Admiral Rogers, since cyber is a relatively new field, it seems like the Services are not having any trouble recruiting talent at this point. However, the issue of retention is of concern to me. If confirmed, what would you recommend for retention of these servicemembers across the total force?

Admiral ROGERS. CYBERCOM remains engaged with each of the Services to address current and projected Active Duty requirements as needed. This includes designating servicemember re-enlistment and career field bonuses for cyber career fields, along with associated Active Duty service commitments to assist with retention. Additionally, the Command continues to utilize civilian temporarily expanded hiring authorities and is in negotiation with the Air Force to expand the current internship program to include universities offering cyber-specific expertise. The National Guard and Reserves offer servicemembers the opportunity to continue contributing to the cyber mission in uniform after they have completed Active Duty service. We will continue to work with the Services to develop plans to integrate the National Guard and Reserves into the cyber domain, including recruitment and retention strategies for Reserve component members.

14. Senator GILLIBRAND. Vice Admiral Rogers, do you believe that current retention strategies are useful to the cyber force, or should we be considering different strategies?

Admiral ROGERS. While to date overall retention has not been a concern, strategically, we will continue to work with the services to address assignment policies and career management for highly technical/highly trained cyber professionals with the desired result to maintain skill currency and utility. Strategies are still being developed/implemented, once implemented, retention rates will be monitored.

JOINT INFORMATION ENVIRONMENT

15. Senator GILLIBRAND. Vice Admiral Rogers, in some of my conversations, I have heard that the Joint Information Environment is a good idea, but there are some concerns about the challenges of implementing it effectively. What challenges do you see, and if confirmed, what would you do to address concerns about implementation?

Admiral ROGERS. The Joint Information Environment (JIE) will transform the DOD Information Network (DODIN) into a defensible and operationally effective architecture by shifting the focus from protection of individual Military Service-specific networks, systems and applications to securing data and its uses. I support the JIE approach. Given these challenges, the threat, and the need for efficiency, we must move in this direction. I see three key challenges to JIE implementation. First, transferring responsibility and authority for network command, control, and security of an organization's operational network to a third party is a new paradigm that

will be challenging to overcome. Second, the Department must leverage finite resources to design and implement JIE while continuing to operate and maintain the existing DODIN infrastructure. JIE will demand the involvement of some of our best technical experts even as we rely on these same people for current operations. Additionally, it will need to include the design and implementation of a strong security infrastructure. Third, implementation of the JIE framework is being accomplished without a program of record and corresponding dedicated funding line. This intentional, strategic decision introduces a degree of complexity in maintaining alignment of the various IT acquisition programs across the Department, but the risk appears to be manageable and will allow the Services and combatant commands to retain control of their individual information technology budgets while providing capabilities that enable the entire enterprise. We are addressing these challenges through a combination of rapid capability implementation and optimization of existing governance constructs. We are leveraging the lessons learned from implementing JIE Increment 1 in U.S. European Command and U.S. Africa Command, streamlining development processes, minimizing the time required of our technical experts, and ensuring critical path activities minimize impact on Department components. Additionally, in partnership with the DOD Chief Information Office, we are leveraging established governance forums to apply the collective expertise of the entire JIE team toward solving tough challenges and making informed decisions.

CIVILIAN CYBER RECRUITING AND RETENTION

16. Senator GILLIBRAND. Vice Admiral Rogers, during the hearing, you identified recruitment and retention of civilian cyber personnel as a greater challenge than recruitment and retention of military cyber personnel. What specifically are the challenges and what do you believe is needed to recruit and retain civilian cyber warriors in DOD?

Admiral ROGERS. We are faced with a couple of recruiting and retention challenges. The recent furlough situation created uncertainty for recruiting prospective new hires and retaining our talented cadre workforce. While Federal employment has traditionally been seen as a secure career, both NSA and CYBERCOM experienced employee turmoil directly attributed to an absence of appropriations at the beginning of fiscal year 2014. Given our close relationship with NSA, many employees experienced the furlough while others did not. This had a negative impact on morale and caused employees to search for perceived "non-furloughed" positions to mitigate their employment risk. This of course results in skewing the workforce mix, and also leads to some critical work roles remaining vacant. We also continue to experience difficulty hiring personnel with the skills we need while competing with industry, academia, and other non-Federal and Federal organizations. We have had success using the "Schedule A Expedited Hiring Authority" that was granted CYBERCOM over the past 3 years and expires 31 December 2014. However, we continue to have great difficulty competing with outside agencies and companies due to the speed at which they can hire and the generally higher level of salary that they can offer.

17. Senator GILLIBRAND. Vice Admiral Rogers, do you see a need for Congress to grant additional authorities to DOD to recruit and retain civilians?

Admiral ROGERS. Yes. In order to address the challenges of recruitment and retention of civilian cyber warriors, CYBERCOM needs additional authorities such as:

(1) Rank-In-Person: The ability to assess and act on the knowledge, skills and abilities (KSA) an individual brings to the job, rather than focusing principally on assessing a position against rigid job classification factors.
(2) Performance Focused Pay: Designed to compensate and reward employees based on performance, contribution or competencies; enhances ability to compete with the private sector for high quality candidates, including college graduates.
(3) Market Informed Pay: Pay ranges tied to pay rates for comparable positions with CYBERCOM's private/public competitors; grade levels replaced with career levels and varied by occupation; OPM classification standards are aligned with CYBERCOM career levels.
(4) Extended Probationary Period: Allows the 1 year probationary period to be extended for up to 3 years determined by the type of work.
(5) Training and Development (Critical Skills): Expanded CYBERCOM authority to provide funding for degree and certificate programs.

In order to stay competitive in the work place and execute the CYBERCOM mission effectively, the Commander, CYBERCOM, needs greater flexibility to recruit, hire and retain a highly skilled work force. Under Title 10 excepted authorities, the Director, NSA/Chief CSS has that flexibility and is thus able to recruit and retain some of the Nation's most talented technical PhDs, Computer Scientists, Engineering and Physical Scientists and Mathematicians, business and support professionals. Commander, CYBERCOM, needs these same authorities to build a similar civilian work force.

In addition, the previous commander in an open hearing identified, ".with respect to personnel, I think we need to come up with a personnel system that puts all of our cyber team in one personnel construct, especially for the NSA CYBERCOM team."

QUESTION SUBMITTED BY SENATOR MAZIE K. HIRONO

CYBERSECURITY VITAL TO NATIONAL SECURITY

18. Senator HIRONO. Vice Admiral Rogers, cybersecurity plays a vital role in the security of our Nation. With $5.1 billion in the fiscal year 2015 budget request, there are many opportunities to incorporate, both Active and Reserve cyber units to play critical roles in cybersecurity. With cybersecurity and intelligence infrastructure already in place on Oahu and many cyber threats originating in the Pacific region, I believe that the Hawaii National Guard would be an ideal candidate to establish a cyber force. Please share your thoughts on the National Guard's role in the cybersecurity mission at the national level as well as specifically for the State of Hawaii?

Admiral ROGERS. Regarding the role of the National Guard, to include the State of Hawaii, in State-specific cyber missions we are looking at two distinct areas of concern. One, we continue to work with the Services on how the National Guard Forces are employed by CYBERCOM specifically, and integrated with the CMF. Second we are looking to develop a CMF capability that included the National Guard and its role in support civil authorities in resiliency, recovery, and aid in investigations. One concept for consideration, subject to appropriate mission analysis, feasibility study, authorities analysis, and requisite DOD approvals, would be to establish cyberspace situational awareness and capabilities for protecting Critical Infrastructure and Key Resources (CIKR) within the States' utilizing the Reserve Force construct. Additionally, we recognize Reserve component civilian experience and certifications are a critical benefit in the quickly evolving cyberspace domain which enhances military based training programs.

QUESTIONS SUBMITTED BY SENATOR JAMES M. INHOFE

NETWORK VULNERABILITY

19. Senator INHOFE. Vice Admiral Rogers, U.S. Transportation Command (TRANSCOM) has been subject to a growing number of cyber attacks. TRANSCOM's reliance on unique contracts—such as the CRAF program where U.S. civil air carriers agree to augment organic military airlift during a crisis in exchange for access to peacetime defense business—creates unique challenges. In a contingency, TRANSCOM's ability to move troops or supplies could be hindered if a vendor's network were compromised. Today there appears to be little sharing of threat and network vulnerability information. Do you share these concerns?

Admiral ROGERS. I do share these concerns, and that is why efforts to enable asset owners to strengthen these networks and hold them accountable are so important. DOD and NSA have long worked to address these issues through voluntary and contractual means including sharing information directly with participating companies in the Defense Industrial Base Cybersecurity/Information Assurance program. DOD further supports broader industry information sharing efforts by providing threat and vulnerability information through DHS. Executive Order 13636 continues to advance information sharing, but legislation is still needed to enhance information sharing among and between private and public entities, and to protect privacy and civil liberties. The end goal is to achieve machine speed cybersecurity and to enable coordinated preventative and response options across the U.S. Government and private sector to protect and defend the United States and our interests in cyberspace.

20. Senator INHOFE. Vice Admiral Rogers, what other unique cybersecurity challenges do you believe we should be aware of?

Admiral ROGERS. The United States faces adversaries that seek persistent presences on military, government, and private networks for purposes such as exploitation and potential disruption and destruction. These adversaries have displayed increasing capacities and sophistication in their capabilities designed to steal, manipulate, and destroy U.S. information and hold our critical infrastructure on which our military and nation rely at risk. This is a constantly changing environment that requires we generate the capability and agility needed to operate in this dynamic environment. In addition to improved information sharing among public and private sector entities, we need to establish timely decision-making structures and processes to provide senior decision makers and operational commanders with a full range of options within the cyber arena. This requires that we partner with our allies, the private sector, within DOD, and across the U.S. Government. These partnerships can assist us in countering common threats and addressing shared vulnerabilities at a larger scale than any one organization can do alone.

21. Senator INHOFE. Vice Admiral Rogers, what steps are TRANSCOM and CYBERCOM taking to address these vulnerabilities?

Admiral ROGERS. Across DOD, we are creating capabilities that can help mitigate these vulnerabilities, but some key capability gaps remain in dealing with highly adaptable and increasingly capable threats. Because the architecture must be agile, secure, reliable and rapidly deployable, DOD is currently involved in efforts to leverage computing technology that can dramatically increase our ability to safely and securely store and access data. In order to create effective cyber teams, we need enough trained and ready cyber experts to perform all the responsibilities; therefore, CYBERCOM is in the process of assembling a workforce that understands how to perform necessary threat management in this domain. We must also have the ability and the confidence to share this common operating picture among government organizations, industry partners, and foreign partners as appropriate. We continue to work across DOD and with other departments and agencies to enact policy changes such as the work under the Executive order that will enhance our ability to strengthen our cybersecurity, but cyber legislation is still needed to enhance information sharing among public and private entities and protect privacy and civil liberties.

22. Senator INHOFE. Vice Admiral Rogers, can TRANSCOM and DOD enact a policy change that can make the fixes that you envision?

Admiral ROGERS. CYBERCOM is collaborating with TRANSCOM and other DOD entities to work with private sector partners to improve network security that will ensure reliable worldwide logistics operations. In the past year, DOD has extensively re-written cybersecurity policies to incorporate National Institute of Standards and Technology (NIST) standards and ensure compatibility across not only the department, but the entire Federal Government. These new policies are currently being disseminated and enacted across DOD, and promise to significantly alter the way DOD evaluates and manages risks across our enterprise. DOD is also working with its U.S. Government counterparts to enact policy and process changes that will enable the coordinated employment of existing homeland security, law enforcement, and military authorities and capabilities, as appropriate. Also, we continue to focus on improving information sharing between the private and public to the greatest extent feasible in the current environment, noting that cybersecurity information sharing legislation would do much to enable and enhance two way real time information sharing.

23. Senator INHOFE. Vice Admiral Rogers, do you feel that TRANSCOM and DOD need more legislative authority to fix this persistent threat brought about by the current cyber intrusion problem?

Admiral ROGERS. The President has the necessary authority to order military action to defend our Nation against all attacks whether they come from terrorists or nation states and in any domain from sea, air, land or cyberspace. Since the President can delegate appropriate authorities to the Secretary of Defense to use the Department's operational capabilities, including CYBERCOM, to defend the Nation from cyber attack, additional legislative authority for DOD or CYBERCOM is not necessary. That said, the operations of TRANSCOM and its close industry partnerships serve to highlight that with so much of the critical infrastructure owned and operated by the private sector, the government has limited visibility and thus is often unaware of the malicious activity targeting our critical infrastructure. These blind spots prevent the Government from being positioned to either help the critical

infrastructure to defend itself or to defend the Nation from an attack, if necessary. This can best be overcome through legislation that removes existing barriers and disincentives and facilitates two-way real time information sharing between the private sector and the government.

QUESTIONS SUBMITTED BY SENATOR KELLY AYOTTE

CYBER DETERRENCE

24. Senator AYOTTE. Vice Admiral Rogers, when DOD endures a cyber attack, how would you characterize our ability to determine who conducted the attack?

Admiral ROGERS. Our ability to determine who conducts cyber attacks depends upon several factors including sophistication of the malicious actors, information sharing capabilities and policies and available trained manpower. Attribution involves an examination of malicious activity based on technical, behavioral, and personal characteristics. Our ability to determine attribution does not solely rely on the mechanical process of geo-location of physical networks or nodes. The possibility always exists the adversary has exploited/hijacked what appears to be the origin and is directing the cyber attacks from a remote location, anywhere in the world. We employ significant resources and manpower to analyze network and intelligence data to determine the true aggressor. Over the past decade, our ability to identify malicious cyber actors has improved significantly as we have adopted a federated approach in the analysis of data necessary to pinpoint the nexus for a given cyber operation. To stay ahead of the adversary, there are currently processes in place to share information and analytic insight across DOD and the Intelligence Community. In addition, defense contractors and other civilian defense organizations have their own sets of information which could lead to the attribution of cyber threat actors and their capabilities and intentions.

25. Senator AYOTTE. Vice Admiral Rogers, how long does it take to identify the attacker?

Admiral ROGERS. Analysis of network traffic is one key element in the attribution process. Analysis of malicious network traffic over time provides valuable clues in the hunt for a nexus in the case of nefarious activity. Developing "signatures" using the aforementioned network analysis techniques, combined with multi-source intelligence information, allows for rapid identification and notification—often within minutes.

The process for identifying top level cyber actors using advanced tools is much more complicated. Attribution can take days to months as the forensic review of the operation is conducted by multiple organizations within DOD and the Intelligence Community. It must be noted, however, that the distributed nature of the Internet combined with the blinding pace in the evolution and growth of cyber tools and associated programs makes timely attribution of the most advanced actors particularly difficult.

26. Senator AYOTTE. Vice Admiral Rogers, how can we improve our attribution capability?

Admiral ROGERS. Attribution of the individuals and/or organizations responsible for malicious cyber activity can run the gamut of difficulty. In order to improve our attribution capability it is imperative we employ highly skilled and trained individuals working with advanced and consistently updated technologies across and between Whole of Government.

Training and recruitment of effective information technology and analysis personnel is critical to building and maintaining an effective cyber force. Our current build-up of National Mission Teams and Cyber Protection Teams are a step in the right direction. It is also important that we continue to strengthen the cyber ranks of existing agencies by hiring the most qualified individuals and providing working environments that are competitive with the private sector.

Substantial investment in research and development of new capabilities by private enterprise, educational institutions, and government agencies is also critical to improving our attribution capability. Attribution capability is highly dependent upon our mastery and dominance of communication and system technologies.

Finally, sharing of malicious cyber activity and associated intelligence across Federal agencies is a key part in the process of understanding the cyber adversary. As attribution models and frameworks continue to mature and are shared and agreed across agencies, each agency's unique insights and information can be shared and organized to deliver more rapid and accurate attribution.

CYBER THREAT

27. Senator AYOTTE. Vice Admiral Rogers, what is your greatest concern in regards to CYBERCOM?

Admiral ROGERS. My greatest concern is dealing with the evolving threat in cyberspace. Our adversaries seek to establish persistent access to military, government, and private-sector networks in order to extract sensitive information and, potentially, to disrupt or destroy critical infrastructure and key resources. As a military and a nation, we are not well positioned to counter such threats. Detecting, containing and expelling capable, persistent intruders can require a commitment of resources and a degree of information sharing and collaboration among government and private-sector entities that is often limited by questions of legal authorities, liability and regulatory necessity.

DOD is improving development of cyber capabilities to detect and respond to the evolving threats; however, key gaps remain. Our legacy information architecture, for instance, is not optimized for defense in its current form and our capability for shared situational awareness across DOD networks are not yet sufficient. We have not yet built trained and ready cyberspace forces in the quantity needed to counter the full range of threats we face. Finally, existing authorities and legal frameworks are not adequate for the public-private threat information sharing and timely responses needed for defense of the Nation in cyberspace. Additional legislation is needed to allow greater public-private information sharing while protecting privacy and civil liberties.

28. Senator AYOTTE. Vice Admiral Rogers, from a DOD perspective, what steps do you think are most important to take in the short-term to better protect our warfighting capability from cyber attacks?

Admiral ROGERS. The most important short-term actions to better protect our warfighting capability mirror DOD's enduring priorities to build a defensible architecture, employ trained and ready CMFs, and maintain global situational awareness and a common operating picture, but with a slightly different order of emphasis. One of my first priorities will be to work closely with NSA and the Services to accelerate the training and deployment of trained and fully qualified personnel to man the CMFs. Effectively employing our CMFs and better focusing their secure and defend efforts requires that we continue to identify and prioritize assets that constitute the critical cyber components or cyber dependencies of our warfighting capabilities. Finally, an improved understanding of critical warfighting cyber components and cyber dependencies is essential for enhancing our efforts to build and maintain global situational awareness in cyberspace.

CYBERCOM AND U.S. NAVY RESERVES

29. Senator AYOTTE. Vice Admiral Rogers, the Military Services provide many of our Nation's cyber professionals. What role do you believe the Reserve component—including the National Guard—should play in cyber operations?

Admiral ROGERS. We are engaged with the Services on the proper role of Reserve component cyber forces. The ability to identify, leverage, and employ these forces can provide a critical enabler for national cyber defense. The Air Force and Army are planning to have the Reserve component forces part of their respective CMF build. These plans are currently being vetted within each of the respective Services.

The Reserve component, to include the National Guard, plays an essential role in physical defense and public security. The cyber mission provides an opportunity for the Services to leverage the dual nature of guardsmen and the complementary nature of reservists to address specific needs, fill gaps and when required, supplement the Active Force in a surge capacity. A significant contribution to the national cyber defense mission is the ability of guardsmen and reservists to leverage their civilian expertise, professional knowledge, and established relationships in order to support Federal, State, or local mission tasks as assigned by appropriate authorities.

30. Senator AYOTTE. Vice Admiral Rogers, what specific role do you think the U.S. Navy Reserves should play in cyber operations?

Admiral ROGERS. Since 2012, the Navy Reserve (NR) fulfills a significant role in Fleet Cyber Command/Commander Tenth Fleet (FCC/C10F) efforts to build and deploy its CMF structure. Reserve personnel are sourced from across all FCC/C10F Reserve units, Selected Reserves, and a mix of volunteers from Voluntary Training Units, a subset of the Inactive Ready Reserve. The FCC/C10F's utilization of Navy Reserve personnel includes the drafting of CMF team-specific Concepts of Operations, as well as the strategy for development and formalization of a plan for the

Active component Navy CMF team build, which is currently under review by FCC/C10F. Additionally, Navy Reserve personnel currently augment headquarters functions on both the cyber plans and targeting, and fires efforts. Navy reservists currently support Active component cyber exercises such as Cyber Flag and Cyber Guard, and serve as a critical force augmentation by providing immediate, trained, and experienced operators.

CYBERSECURITY AND THE PRIVATE SECTOR

31. Senator AYOTTE. Vice Admiral Rogers, under the cybersecurity Executive order that President Obama signed in February 2013, the Government was tasked with improving the manner in which it shares information with the private sector. From a cyber perspective, how would you assess the information flow between the U.S. Government and the private sector?

Admiral ROGERS. In the last few years, and most recently under Executive Order 13636, the U.S. Government has made important progress in providing information to the private sector. Notable examples include the Enhanced Cybersecurity Services program for sharing threat and technical information from the Government to critical infrastructure sectors, and the release in February 2014 of the Cybersecurity Framework. Yet, without two-way sharing between the private sector and the Government, the Government may not have insight to malicious cyber activities within privately owned and operated networks in time to enable the private sector to defend itself, or to defend the United States, if necessary.

32. Senator AYOTTE. Vice Admiral Rogers, does the Government share enough information with the private sector?

Admiral ROGERS. No, despite the recent progress, there is room for improvement in what cybersecurity information the U.S. Government shares with the private sector, as well as what the private sector shares with the U.S. Government. The U.S. Government needs to improve its information sharing policies and processes in a manner that is timely, respects privacy and civil liberties, is sensitive to competitive advantage concerns, and protects intelligence and law enforcement sources, methods, operations, and investigations.

33. Senator AYOTTE. Vice Admiral Rogers, if confirmed as Director of the NSA and Commander of CYBERCOM, what more would you do to have a better flow of information to private sector companies so they can best protect their systems from cyber attacks?

Admiral ROGERS. As the Commander, CYBERCOM and the Director, NSA/Chief CSS, I will partner with DOD, DHS, FBI, and the Office of the Director of National Intelligence to improve machine-speed cybersecurity information sharing with the private sector. To this end, I will continue to support the goals of Executive Order 13636, namely: provide threat information to DHS, DOD, and other sector-specific agencies; assist in expanding the DHS-managed Enhanced Cybersecurity Services program to all critical infrastructure sectors; and move expeditiously to implement secure sharing of classified cybersecurity information with appropriately cleared private entities.

34. Senator AYOTTE. Vice Admiral Rogers, on the flip side, when a defense company endures a cyber attack, is that being shared with DOD? In other words, do we really understand the degree to which our defense industrial base is under cyber-attack?

Admiral ROGERS. The Department is adapting its DOD–Defense Industrial Base Voluntary Cybersecurity/Information Assurance (DIB CS/IA) Activities program (32 CFR Part 236) to incorporate mandatory incident reporting requirements under section 941 (NDAA for Fiscal Year 2013) while maintaining the voluntary cyber threat information sharing. This amended program will strengthen DOD's ability to safeguard DOD information on contractor unclassified information systems and provide contractors increased incentive to join the voluntary DIB CS/IA program for more robust cybersecurity collaboration with DOD. However, all stakeholders in the public and private sectors will remain disadvantaged in understanding the full scope of the threat without legislation to enhance information sharing among and between private and public entities while protecting privacy and civil liberties and clarifying liability and anti-trust issues.

35. Senator AYOTTE. Vice Admiral Rogers, countless jobs, investments, and dollars are being lost from the theft of intellectual property each year due to cyber hacks. How can we help our defense industrial base better protect itself?

Admiral ROGERS. I agree that the theft of intellectual property is a real and growing problem that negatively impacts the technological competitiveness, economic health, and national security of the United States. Several initiatives are underway to help the Defense Industrial Base (DIB) better protect itself. Cybersecurity information sharing occurs within the voluntary DIB Cybersecurity and Information Assurance (DIB CS/IA) Program and its optional DHS-managed Enhanced Cybersecurity Services (ECS) component. In addition, DOD, as the Sector Specific Agency for the DIB, works with DHS to implement the National Infrastructure Protection Program sector partnership model and risk management framework. While these partnerships help to improve the security of the DIB, and improve our collective strength against the theft of our Nation's intellectual property, additional steps are needed to remove barriers to cybersecurity information sharing and encourage industry to harden its networks.

INTERAGENCY INFORMATION SHARING

36. Senator AYOTTE. Vice Admiral Rogers, what role should CYBERCOM play in coordinating with other agencies such as DHS to make sure the U.S. Government has a common picture of the threat and can develop a well-coordinated response?

Admiral ROGERS. As part of the Comprehensive National Cybersecurity Initiative (CNCI), Federal cybersecurity operations centers across the U.S. Government were linked to foster improved information sharing and shared situational awareness of cyber threats. CYBERCOM's Joint Operations Center is and should continue to be a key member facilitating that linkage across the whole of government, particularly when DOD is the designated lead for a cyber-related operation. In those circumstances where another agency has the lead, then CYBERCOM should act in a supporting capacity, as needed.

It is important to note that developing well-coordinated responses to potential cyber incidents begins long before an incident comes to light. Ideally, the U.S. Government would have pre-coordinated response options to cyber incidents available to respond to the most likely and most dangerous cyber threats. This requires advanced planning, capability development, machine-speed information sharing, whole-of-government exercises, and timely and agile decision-making processes that allow national leaders to assess and manage risks both during steady state and crisis operations. CYBERCOM is—as part of a broader DOD and U.S. Government effort—well-suited to support the development and exercise of pre-coordinated response options needed to defend the United States and its interests in cyberspace.

37. Senator AYOTTE. Vice Admiral Rogers, based on your preparation for your nomination hearing, how would you characterize CYBERCOM's current relationship with DHS?

Admiral ROGERS. CYBERCOM's relationship with DHS is good and growing. DHS, the lead for national protection, is a key partner to DOD, the lead for national defense. Efforts to protect and defend the United States and its interests in cyberspace must go hand-in-hand. As the nature of conflict and competition in cyberspace evolves, so, too, must CYBERCOM's relationship with DHS in order to ensure our Nation's ability to operate, defend, and protect ourselves in the domain. CYBERCOM's relationship with DHS will continue to grow both in importance and strength over the coming months and years. I look forward to working with my DHS counterparts to this end.

[The nomination reference of VADM Michael S. Rogers, USN, follows:]

NOMINATION REFERENCE AND REPORT

AS IN EXECUTIVE SESSION,
SENATE OF THE UNITED STATES,
January 30, 2014

Ordered, That the following nomination be referred to the Committee on Armed Services:

The following named officer for appointment to the U.S. Navy to the grade indicated while assigned to a position of importance and responsibility under Title 10, U.S.C., section 601:

To be Admiral.

VADM Michael S. Rogers, USN, 9688.

[The biographical sketch of VADM Michael S. Rogers, USN, which was transmitted to the committee at the time the nomination was referred, follows:]

RÉSUMÉ OF SERVICE CAREER OF VADM MICHAEL SCOTT ROGERS, USN

28 Aug 1981	Ensign
28 Aug 1983	Lieutenant (junior grade)
01 Sep 1985	Lieutenant
01 Sep 1991	Lieutenant Commander
01 Sep 1997	Commander
01 Sep 2002	Captain
02 Nov 2007	Designated Rear Admiral (lower half) while serving in billets commensurate with that grade
01 Feb 2008	Rear Admiral (lower half)
01 Oct 2010	Rear Admiral
30 Sep 2011	Vice Admiral, Service continuous to date

Assignments and duties:

	From	To
NROTC Unit Auburn University (Asst Admin Officer)	Aug 1981	Sep 1981
USS *Caron* (DD 970) (Acting Division Officer)	Sep 1981	Dec 1981
Surface Warfare Officers School Command, Newport, RI (DUINS)	Jan 1982	May 1982
Naval Justice School, Newport, RI (DUINS)	May 1982	Jun 1982
USS *Caron* (DD 970) (Combat Information Center Officer) (Anti-Submarine Warfare Officer)	Jun 1982	Jan 1985
Commander, Naval Military Personnel Command, Washington, DC (Navy Affirmative Action Plan Manager)	Feb 1985	Nov 1986
Naval Security Group Dept, Naval Comm Station, Spain (Surface/Subsurface Direct Support Officer) (Electronic Warfare Officer)	Nov 1986	Dec 1989
Commander, U.S. Atlantic Fleet (Assistant Shore and National Cryptologic Systems Officer)	Jan 1990	Jan 1993
Armed Forces Staff College (Student)	Jan 1993	Apr 1993
Naval Technical Training Center, Pensacola, FL (Student)	May 1993	May 1993
Commander, Carrier Group Two (Staff Cryptologist)	Jun 1993	May 1995
Bureau of Naval Personnel, Washington, DC (Cryptologic Junior Officer Detailer)	May 1995	May 1997
Commander, Naval Security Group Command (Executive Assistant)	May 1997	Jun 1998
CO, Naval Security Group Activity, Winter Harbor, ME	Jul 1998	Jul 2000
Commander, Sixth Fleet (Fleet Information Operations and Cryptology Officer)	Jul 2000	Jul 2002
National War College (Student)	Jul 2002	Jun 2003
Joint Staff (Head, Computer Network Attack/Defense Branch)	Jun 2003	Oct 2003
Joint Staff (Chief, Information Operations Division)	Oct 2003	Feb 2004
Joint Staff (Executive Assistant, Director for Operations) (J–3)	Feb 2004	Aug 2004
Joint Staff (Executive Assistant, Director, Joint Staff)	Aug 2004	Aug 2005
Joint Staff (Special Assistant to CJCS/Director, Chairman's Action Group)	Aug 2005	Nov 2007
Commander, U.S. Pacific Command (Director for Intelligence) (J2)	Dec 2007	Sep 2009
Joint Staff (Director for Intelligence) (J2)	Sep 2009	Sep 2011
Commander, Fleet Cyber Command/Commander, 10th Fleet	Sep 2011	To date

Medals and awards:

Defense Superior Service Medal with two Bronze Oak Leaf Clusters
Meritorious Service Medal with two Gold Stars
Joint Service Commendation Medal
Navy and Marine Corps Commendation Medal with one Silver Star
Joint Meritorious Unit Award with three Bronze Oak Leaf Clusters
Navy Unit Commendation
Meritorious Unit Commendation with two Bronze Stars
Navy "E" Ribbon

Navy Expeditionary Medal with three Bronze Stars
National Defense Service Medal with one Bronze Star
Armed Forces Expeditionary Medal with one Bronze Star
Global War on Terrorism Expeditionary Medal
Global War on Terrorism Service Medal
Military Outstanding Volunteer Service Medal
Sea Service Deployment Ribbon with two Bronze stars
Overseas Service Ribbon with four Bronze Stars
Expert Rifle Marksmanship Medal
Expert Pistol Shot Medal

Special qualifications:

BS (Business Administration) Auburn University, 1981
MS (National Security Strategy) National Defense University, 2003
Designated Surface Warfare Officer, 1983
Designated Cryptologic Officer (Information Warfare), 1986
Designated Joint Qualified Officer, 2006
Designated Level IV Joint Qualified Officer, 2009
CAPSTONE 2009–4 13JU
Pinnacle 2012–1

Summary of joint duty assignments:

Assignment	Dates	Rank
Joint Staff (Head, Computer Network Attack/Defense Branch)	Jun 03–Oct 03	CAPT
Joint Staff (Chief, Information Operations Ops Division)	Oct 03–Feb 04	CAPT
Joint Staff (Executive Assistant, Director of Operations, J–3)	Feb 04–Aug 04	CAPT
Joint Staff (Executive Assistant, Director, Joint Staff)	Aug 04–Aug 05	CAPT
Joint Staff (Special Assistant to CJCS/Director, Chairman's Action Group)	Aug 05–Nov 07	CAPT
Commander, U.S. Pacific Command (Director for Intelligence) (J2)	Dec 07–Sep 09	RDML
Joint Staff (Director for Intelligence) (J2)	Sep 09–Sep 11	RDML/RADM

[The Committee on Armed Services requires certain senior military officers nominated by the President to positions requiring the advice and consent of the Senate to complete a form that details the biographical, financial, and other information of the nominee. The form executed by VADM Michael S. Rogers, USN, in connection with his nomination follows:]

UNITED STATES SENATE

COMMITTEE ON ARMED SERVICES

Room SR–228

Washington, DC 20510–6050

(202) 224–3871

COMMITTEE ON ARMED SERVICES FORM

BIOGRAPHICAL AND FINANCIAL INFORMATION REQUESTED OF NOMINEES

INSTRUCTIONS TO THE NOMINEE: Complete all requested information. If more space is needed use an additional sheet and cite the part of the form and the question number (i.e. A–9, B–4) to which the continuation of your answer applies.

PART A—BIOGRAPHICAL INFORMATION

INSTRUCTIONS TO THE NOMINEE: Biographical information furnished in this part of the form will be made available in committee offices for public inspection prior to the hearings and will also be published in any hearing record as well as made available to the public.

1. **Name:** (Include any former names used.)
Michael S. Rogers.

2. **Position to which nominated:**
Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command.

3. **Date of nomination:**
January 30, 2014.

4. **Address:** (List current place of residence and office addresses.)
[Nominee responded and the information is contained in the committee's executive files.]

5. **Date and place of birth:**
October 31, 1959; Chicago, IL.

6. **Marital Status:** (Include maiden name of wife or husband's name.)
Married to Dana M. Rogers (Maiden Name: Walck).

7. **Names and ages of children:**
Justin, age 25.
Patrick, age 21.

8 **Government experience:** List any advisory, consultative, honorary or other part-time service or positions with Federal, State, or local governments, other than those listed in the service record extract provided to the committee by the executive branch.
None.

9. **Business relationships:** List all positions currently held as an officer, director, trustee, partner, proprietor, agent, representative, or consultant of any corporation, firm, partnership, or other business enterprise, educational, or other institution.
None.

10. **Memberships:** List all memberships and offices currently held in professional, fraternal, scholarly, civic, business, charitable, and other organizations.
Member, U.S. Naval Institute
Member, Auburn University Alumni Association

11. **Honors and awards:** List all scholarships, fellowships, honorary society memberships, and any other special recognitions for outstanding service or achievements other than those listed on the service record extract provided to the committee by the executive branch.
None.

12. **Commitment to testify before Senate committees:** Do you agree, if confirmed, to appear and testify upon request before any duly constituted committee of the Senate?
Yes.

13. **Personal views:** Do you agree, when asked before any duly constituted committee of Congress, to give your personal views, even if those views differ from the administration in power?
Yes.

[The nominee responded to the questions in Parts B–E of the committee questionnaire. The text of the questionnaire is set forth in the Appendix to this volume. The nominee's answers to Parts B–E are contained in the committee's executive files.]

SIGNATURE AND DATE

I hereby state that I have read and signed the foregoing Statement on Biographical and Financial Information and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

MICHAEL S. ROGERS.

This 16th day of January, 2014.

[The nomination of VADM Michael S. Rogers, USN, was reported to the Senate by Chairman Levin on March 16, 2014, with the recommendation that the nomination be confirmed. The nomination was confirmed by the Senate on March 31, 2014.]