HEARING TO CONSIDER THE 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.

Committee staff members present: Peter K. Levine, staff director; and Leah C. Brewer, nominations and hearings clerk.

Majority staff members present: Joseph M. Bryan, professional staff member; Richard W. Fieldhouse, professional staff member; Creighton Greene, professional staff member; Jason W. Maroney, counsel; Thomas K. McConnell, professional staff member; and Mariah K. McNamara, special assistant to the staff director.

Minority staff members present: John A. Bonsell, minority staff director; Daniel C. Adams, minority associate counsel; Steven M. Barney, minority counsel; William S. Castle, minority general counsel; Samantha L. Clark, minority associate counsel; Anthony J. Lazarski, professional staff member; Daniel A. Lerner, professional staff member; and Sean J. Wolfe, research analyst.

Staff assistants present: Daniel J. Harder and Alexandra M. Hathaway.

Committee members' assistants present: Carolyn A. Chuhta, assistant to Senator Reed; Cathy Haverstock, assistant to Senator Nelson; Jennifer H. Barrett and Christopher R. Howard, assistants to Senator Udall; David J. LaPorte, assistant to Senator Manchin; Karen Courington, assistant to Senator Kaine; Stephen M. Smith, assistant to Senator King; Paul C. Hutton IV and Brian J. Rogers,

assistants to Senator McCain; Lenwood A. Landrum, assistant to Senator Sessions; C. Stephen Rice, assistant to Senator Chambliss; Joseph G. Lai, assistant to Senator Wicker; Bradley L. Bowman, assistant to Senator Ayotte; Craig R. Abele, assistant to Senator Graham; Joshua S. Hodges, assistant to Senator Vitter; Robert C. Moore, assistant to Senator Lee; and Victoria Coates and Jeremy H. Hayes, assistants to Senator Cruz.

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), and the nomination of Admiral Michael Rogers to be Commander, U.S. Cyber Command (CYBERCOM), Director of—and Director of the National Security Agency, 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 31st 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, 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 the Department of Defense. 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 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, quote—and this is the board saying this, that they have not, quote, "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? And 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.

So 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 CENTCOM and 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.

So 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 always 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 his—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 note, wonderful introduction.

The first question we're going to ask Admiral Rogers is what did he know about you in homework—in home room. I think 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, NOMINATED 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 U.S. Transportation Command.

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 the U.S. Transportation Command, 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, chairman.

[The prepared statement of General Selva follows:]

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, NOMINATED 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. 30 years ago, one evening, 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 at 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, U.S. Cyber Command, 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 the Department of Defense and agencies and organizations across the U.S. Government as well as the Congress.

I am also mindful that CYBERCOM and 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 National Security Agency 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 National Security Agency and the U.S. Cyber Command, 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 Cyber Command and 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.

[The prepared statement of Admiral Rogers follows:]

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 con-

sult 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 seven minutes for our first round.

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 U.S. Transportation Command consists significantly of our relationship with commercial transportation and logistics providers. So roughly 90 percent of the information in my current position as Air Mobility Command, and I suspect inside Transportation Command 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. Do you agree that the government, first of all—no, 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 par-

ticular would be the idea of speed, the ability to query the data, to work with 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. And the Oversight Board said that, quote, "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."

Do you have an assessment of how—first of all, 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 National Security Agency 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—or do you have, yes, 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 the Department of Defense 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 U.S. Cyber Command, 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.

So 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 four 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.

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

Admiral ROGERS. Yes, sir, it did.

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

Admiral ROGERS. Well, 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 I guess TRANSCOM had doubled from 45,000 in 2011 to nearly 100,000 in 2012. Now, that's not very good, is it? I mean, 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.

So 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. So if confirmed for the position of TRANSCOM Commander, I'll continue to work that issue hard with General 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. Well, all right. When we had a hearing on February 27th, General Alexander—and 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.

Do you think, Admiral Rogers, that—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. That "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. Well, 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. Well, 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, quote, "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.

And now this new capability—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 advanced 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, quote, "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 9–11 and I want to set the record straight from my point of view. As the 9/11 Commission pointed out, the CIA knew about Al-Midhar, but did not tell the FBI. 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 FISA Act. The committee asked your understanding of the legal rationale for 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 DNI.

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. Now, 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.

Senator UDALL. You——

Admiral ROGERS. 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. And 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, I want to—and I don't want to steal Senator McCain's thunder, although that's impossible, to steal Senator McCain's thunder. But 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.

But in a more specific context, you noted in your comments that we've got 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. But 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've got to make those investments up front. 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, as you know, 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. Quote: "'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. So 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. And the damage done in your view was 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, well, what if they had decided that was their intent?

Senator MCCAIN. I thank you.

Admiral, we've got 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. I quote

from—there were polls in the January Quinnipiac Survey. 57 percent of Americans branded Mr. Snowden as a, quote, "whistleblower." 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 many—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 got 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 National Security Agency. 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 up front 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. So you do appreciate the fact that we have, at least with a large number of Americans and people around the world, a significant problem with the PR 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. Well, if I had a recommendation for you it would be as much as possible, given the aspects of national security, that you maybe 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, as you know, 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.

So 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. And frequently those members of the Naval Reserve or of the National Guard, the Army National Guard or Air Force, 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, if I can, 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 Austin 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 intel community that we might have picked up on that. So 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 National Security Agency, 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've got 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. Well, you're exactly right. It's truly unfortunate that General Alexander was put out there kind of 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 o 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.

But the fact that the administration did not give General Alexander the kind of support they should is really pretty, pretty disturbing on my part, and I'm very hopeful—and again, 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. As you know, we've been working on a cyber-bill for years now. We're getting very close to an agreement within the Intelligence Committee between the chairman and myself on a cyber-bill that is much needed. One of the key provisions and kind of the last remaining obstacle we've got 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. And 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. So 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. So 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. Well, as the nominee I haven't done that for Cyber Command or NSA, sir. But if——

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 what policies—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. I guess again 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 government 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. And I guess, 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? I guess 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. But I guess 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 that 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 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. So 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.

Let me just start, 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 U.S. 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, as you know, as 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.

So I wanted to ask you, in your role as commander-to-be, Air Mobility Command, what's your assessment of the 157th Air Refueling Wing, 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 also wanted to ask you—I noted Senator Donnelly asked you about the issue of—I don't know how specifically he got into it—of the Northern Distribution Network with regard to our retrograde from Afghanistan. In light of what's happening in the Ukraine, we are—as you know, 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. So 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. So 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 assessing—accessing, excuse me, 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 it's 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 the Department of Defense'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, quote: "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 capabili-

ties 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 got 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 JIE, the Joint Information Environment, I think is so critical to the future for us. We have got to get to a defensible architecture.

Senator AYOTTE. We've got to work with you on that.

Finally, let me just—you know, there's been a lot of discussion about Edward Snowden here today. Do you believe that the disclosures that he made have put American—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. So 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.

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? And how about the vulnerability of commercial carriers to events like cyber intrusions? What do you see—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. So 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, would be brought to us by our commercial partners. I don't know have the specific statistics.

Senator KING. As the demands of Afghanistan diminish, is there kind of 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 Civil Reserve Air Fleet 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. So 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 three-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 Intelligence and in this committee on cyber issues, Cyber Command, 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. I say that—right now, in my current duties on the Navy I work for General Alexander both as U.S. Cyber Command and as NSA, 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've got to be a spokesman, you've got 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've got to change the current dynamic.

Senator KING. Well, 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—my father used to say if you drove straight at the Pentagon it kept getting further and further away. I kind of 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 kind of 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've got to get to some idea of deterrence within the cyber arena.

Senator KING. I think you're absolutely right about that, and deterrence—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 visiting 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 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 National Security Agency does. We are given, if confirmed—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 available 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'm not—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 National Security Agency, 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?

Senator LEE. 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. And 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.

And 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 for your—congratulate you on your nominations. I've read your resumes, quite impressive. And thank you for the service to our great country.

Also I want to acknowledge the passing on Sunday March 9th 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?

And 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. From the standpoint of coming from—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. But in—

Senator MANCHIN. Is that because of security?

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

Senator MANCHIN. Could you maybe get some information on that?

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

[The information referred to follows:]

[COMMITTEE INSERT]

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. So 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. I will, if confirmed—

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

General SELVA.—I will get with the DLA team and get you that information.

[The information referred to follows:]

[COMMITTEE INSERT]

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 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 if—I would assume there has been. So if you can do that, I'd appreciate it, sir.

Also, as you know, 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. Are we taking active—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 kind of 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 know, 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 U.S. Cyber Command 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 Cyber Command side and the National Security Agency side for the last two and a half 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. I mean, 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 National Security Agency chain of command, there are avenues both with an inspector general structure, both within NSA and U.S. Cyber Command 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. So you would 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. 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 eight 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 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. So there is a big of a two-sided coin there on the impact of sequestration on the readiness of that fleet, 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 over the last ten years?

General SELVA. Senator, we've had a fairly high OPSTEMPO, 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. Well, 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? And 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 Al-Qaeda—that we're at war with Al-Qaeda and their affiliates?

Admiral ROGERS. Yes, sir. And 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 9–11?

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. But 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 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. So 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:]

[COMMITTEE INSERT]

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 adopt, 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. And that 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. Well, thank you very much, Mr. Chairman. And 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 Civil Reserve Air Fleet. I know

you're undergoing—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, on 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 Civil Reserve Air Fleet we have, as you know, 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. So part of the study was to get at the eaches of how the industry runs and get at the broad macroeconomics of how the industry is going to evolve over time.

So 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 Civil Reserve Air Fleet. As you may be aware, the policy that governs how we manage, National Airlift Policy, was last updated in 1987. So 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, Cyber Command, which is a DOD function, and NSA. In your organization are you going to have or contemplate or have now deputies, 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's no changes at this time in those deputies?

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

Senator REED. And 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 Cyber Command, NSA, Homeland Security, every other agency, which basically would give us some—confirm what we believe and maybe 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 the 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. Well, 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. Again—and 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, because in fact we discovered, by the way, 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. And 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 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.

I guess the official announcement came yesterday. I have a news report from WLOX of Biloxi, MS, which says Keesler Air Force Base will lose ten aircraft from the 403rd Wing under proposed defense cuts presented to Congress Monday. The Air Force Reserve Command plans to transfer the ten 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 his own, 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. But 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 fiscal yearDP for savings.

Senator WICKER. Okay. Is there going to be any 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. And I want you to be able to look us in the eye on this committee, General, and assure us that not one dollar 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.

[The information referred to follows:]

[COMMITTEE INSERT]

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

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. So will you—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. So 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. And 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.

Senator Vitter.

By the way, let me interrupt just for one second. The first vote has now begun. I believe it's the first of four that are still scheduled. So I'll be—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. Okay, 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 developing norms within the cyber arena. That's going to be much broader than just U.S. Cyber Command, but clearly Cyber Command I believe is part of that dialogue.

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

Admiral ROGERS. Yes, sir.

Senator VITTER. Okay. In your statement——

Admiral ROGERS. And——

Senator VITTER. Sorry. Go ahead.

Admiral ROGERS. I apologize. 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, quote: "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 wouldn't—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.

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, Cyber Command 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, U.S. Cyber Command currently has an ongoing series of exercises designed to exercise with Guard units in the cyber arena. U.S. Cyber Command 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've got to maximize that capability.

Senator VITTER. Well, I would underscore and encourage that with regard to Cyber Command 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. So 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 specific smarter on to be prepared to discuss very publicly. I think that's an important part of that public discussion.

Senator VITTER. Well, 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:]

[COMMITTEE INSERT]

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.

And 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 kind of got 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.

So 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? And 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 just feel like the challenge about limiting these NSA programs or trying to find the right balance between fighting terrorism, stop-

ping 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 UN 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 and how that then—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. So 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 out 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. So just 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. Well, 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.

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 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 the 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.

But 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 Cyber Command, 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. Well, 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 potential 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 Cyber Command it takes a real balance of service branch personnel, but also DOD civilians.

Admiral ROGERS. Yes, sir.

Senator KAINE. And there's got to be a good mixture.

Admiral ROGERS. Yes, sir.

Senator KAINE. 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.

I guess 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. Well, that's the problem. There's not a lot of 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 you next year. We talk about a weapon, we talk about a delivery system, they understand that, but not cyber attack. And I look at this and I just think that the Senator from Virginia was really onto something. You know, 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. So 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 National Security Agency, 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 National Security Agency.

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. Well, 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. Well, I would ask after this hearing if you would follow up and answer that question in writing, and you can certainly consult 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. So I would appreciate your expanded answer in writing after this hearing.

[The information referred to follows:]

[COMMITTEE INSERT]

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. And 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. Well, 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. So 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.

And 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. Well, 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 if 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.]