NOMINATIONS OF VADM JAMES A. WINNEFELD, JR., USN, TO BE ADMIRAL AND COMMANDER, U.S. NORTHERN COMMAND/ COMMANDER, NORTH AMERICAN AEROSPACE DEFENSE COMMAND; AND LTG KEITH B. ALEXANDER, USA, TO BE GENERAL AND DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE/COMMANDER, U.S. CYBER COMMAND″

THURSDAY, APRIL 15, 2010

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

The committee met, pursuant to notice, at 9:36 a.m. in room SD–G50, Dirksen Senate Office Building, Senator Carl Levin (chairman) presiding.

Committee members present: Senators Levin, Lieberman, Reed, Udall, Hagan, Burris, Kaufman, McCain, and Thune.

Other Senator present: Senator Barbara Mikulski.

Committee staff members present: Richard D. DeBobes, staff director; and Leah C. Brewer, nominations and hearings clerk.

Majority staff members present: Richard W. Fieldhouse, professional staff member; Creighton Greene, professional staff member; Jessica L. Kingston, research assistant; Peter K. Levine, general counsel; and Thomas K. McConnell, professional staff member.

Minority staff members present: Joseph W. Bowab, Republican staff director; Adam J. Barker, research assistant; Paul C. Hutton IV, professional staff member; Michael V. Kostiw, professional staff member; and David M. Morriss, minority counsel.

Staff assistants present: Paul J. Hubbard and Kevin A. Cronin.

Committee members' assistants present: James Tuite, assistant to Senator Byrd; Christopher Griffin, assistant to Senator Lieberman; Gordon I. Peterson, assistant to Senator Webb; Jennifer Barrett, assistant to Senator Udall; Nathan Davern, assistant to Senator Burris; Halie Soifer, assistant to Senator Kaufman; Anthony J. Lazarski, assistant to Senator Inhofe; Sandra Luff, assistant to Senator Sessions; Jason Van Beek, assistant to Senator Thune; and Kyle Ruckert, assistant to Senator Vitter.

OPENING STATEMENT OF SENATOR CARL LEVIN, CHAIRMAN

Chairman LEVIN. Good morning, everybody. The committee meets today to consider the nominations of two senior officers to serve in important command positions. Vice Admiral James Winnefeld, Jr., has been nominated for promotion to the rank of Admiral, to be Commander of U.S. Northern Command and Commander of the North American Aerospace Command, NORAD. Lieutenant General Keith Alexander has been nominated for promotion to the rank of General and to be Director of the National Security Agency, the Director of the Central Security Service, and to be Commander of the new U.S. Cyber Command.

We welcome both our nominees and we thank them, we thank their families, for their long and distinguished service that they've already provided to the Nation. We thank them both also for their willingness to continue serving our Nation in these senior military positions for which they are so well qualified.

Vice Admiral Winnefeld has had a long and distinguished naval career, including a number of joint duty assignments. He has commanded the U.S. Sixth Fleet, NATO Striking and Support Forces, and Carrier Strike Group 2. He is currently serving as the Director of Strategic Plans and Policy, J–5, on the Joint Staff.

U.S. Northern Command, which Admiral Winnefeld has been nominated to lead, was created following the terrorist attacks of September 11, 2001. It is charged with two primary missions, defense of the United States and providing defense support to civil authorities in circumstances where the Federal Government is needed to respond to natural or manmade disasters in the homeland. This later mission requires a high level of cooperation and coordination with other Federal agencies and State agencies, especially the Department of Homeland Security.

The Commander of Northern Command is also dual-hatted as the Commander of NORAD, our binational command with Canada that provides aerospace warning and control and since 2006 maritime warning for North America. NORAD has been a key link between our two nations for more than 50 years.

In addition to Canada, Mexico is also in the Northern Command area of responsibility. Given the continuing high level of drug-related violence in Mexico and the attendant risks to our southern border region, the administration has been focusing high-level attention on Mexico. This future close cooperation between our countries in this and many other matters is critically important to both our countries.

Finally, Northern Command is the combatant command responsible for the operation of the ground-based midcourse defense, GMD, system that has interceptors deployed in Alaska and California to defend our Nation from limited long-range missile attack. That system has been of considerable interest to this committee for a number of reasons, including that we need it to be tested in a way that will give us confidence in its operational effectiveness.

General Alexander too has had a long and distinguished career in military intelligence. He has served as the Director for Intelligence, J–2, for the Central Command and Commanding General for the Army Intelligence and Security Command and the Deputy

Chief of Staff of the Army for Intelligence before becoming Director of the National Security Agency in 2005.

With respect to the position to which General Alexander has been nominated, the creation of a new combatant command, even at the sub-unified level, is an extremely important matter. The creation of a Cyber Command in particular warrants careful scrutiny on the part of this committee for a variety of reasons. CYBERCOM is to be formed solely around the mission involving the relatively sudden dominance of the new computer and communications technology of our age, technology that is ubiquitous, rapidly evolving, and fraught with both great promise and new perils for the country and the world.

As the committee's examination has confirmed, capabilities to operate in cyber space have outpaced the developing of policy, law, and precedent to guide and control those operations. This policy gap is especially concerning because cyber weapons and cyber attacks potentially can be devastating, approaching weapons of mass destruction in their effects, depending on how they are designed and used.

Coupled with the fact that the United States economy and government are the most dependent in the world on the Internet and are therefore the most vulnerable to attacks, the Nation must not only invest in the effectiveness of its defense, but think carefully about the precedents that it sets, hopefully acting wisely in ways that we will accept if others act in the same or similar ways.

Combatant commanders respond to attacks that affect our forces and their ability to execute their missions. The implications of their responses are usually limited and pertain to the theater in which forces are operating. But responses and initiatives in cyber space could have extremely broad and damaging consequences and in the future may require rapid decisionmaking. In this context, some have expressed concern about an officer without strong career experience in commanding combat forces serving as a sub-unified combatant commander.

Faced with that complex situation, the committee proceeded methodically to gain an understanding of what the Congress is being asked to approve and what the key cyber space issues are that need to be addressed. Committee staff have held numerous meetings with senior Department of Defense officials on a host of policy and operational issues associated with CYBERCOM and military and intelligence operations in cyber space. Committee members held a classified meeting with the Vice Chairman of the Joint Chiefs of Staff, General Cartwright, and the Principal Deputy Under Secretary of Defense for Policy, Dr. Jim Miller. The committee posed a lengthy set of policy questions to be answered in writing by the nominee in advance of today's hearing and followed that up with additional meetings and discussions, including with General Alexander.

The committee has been assured that the Department of Defense leadership and the administration as a whole is committed to rapidly closing the cyber space policy gap. The committee has also been assured that the Defense Department is proceeding with appropriate caution and care regarding military operations in cyber space.

We look forward to hearing from our witnesses. There's a possibility that a closed session will be required and if so that session will be held in the Office of Senate Security in the Visitors Center of the Capitol.

Before we turn to our wonderful colleague Senator Mikulski to introduce General Alexander, let me call on Senator McCain for his opening comments.

STATEMENT OF SENATOR JOHN MCCAIN

Senator MCCAIN. Thank you very much, Mr. Chairman. I join you in welcoming Lieutenant General Alexander and Vice Admiral Winnefeld and their families.

General Alexander, the U.S. Cyber Command was established, as we all know, by the Secretary of Defense last year. Since then I have shared the concerns of Senator Levin and others about ensuring that the role, mission, legal authorities, and rules of engagement that Cyber Command will employ are well thought out and understood. I think we've made progress in achieving greater clarity in this regard and that you are well qualified for this new assignment.

The Department must have a centralized command to address the challenges of cyber warfare, to provide the support to the regional combatant commands, and ensure that the Department of Defense, while focused on its own military networks and information grid, also is ready, if directed by the President, to assume a position of leadership and support to civilian authorities in this regard.

Continuing intrusions and attacks by difficult to identify and locate actors on our civilian and military networks and web sites demand not only a robust defensive capability, but the ability to respond offensively when the circumstances call for it. One need only consider the examples of cyber warfare conducted against the Republic of Georgia in 2008 and Estonia in 2006 to appreciate the nature of this form of modern warfare.

We look forward to your testimony about how Cyber Command will function in protecting our vital national assets and infrastructure. I also noted in the media this morning that you believe there are certain gaps in legislative form and also in regulations that need to be improved in order to help you complete your mission successfully and under the legal framework that you feel is necessary. I look forward to hearing from you on that aspect of your new responsibilities.

Admiral Winnefeld, I congratulate you on your nomination to head U.S. Northern Command and North American Aerospace Defense Command. The vicious attacks of 9–11 are never far from our thoughts and ensuring that effective support of civilian authorities should be among our highest priorities. The same is true, of course, for natural disasters, which demand a capable, tested, intergovernmental response in which Northern Command is a key player.

Admiral Winnefeld, I want to particularly emphasize the continuing growing threat to our National security posed by the violence along our border with Mexico. Your answers to the committee's advance questions about the importance of combatting drug trafficking and drug violence reflect my deep concerns about the

corrosive effect of this plague on both the United States and Mexico. As you know, the drug-related violence in Mexico is appalling. As you noted, there were over 6500 drug-related murders in Mexico last year. So far this year, there have been nearly 2,000 deaths resulting from drug-related violence. Last month, the murders in Juarez of Lesley Enriquez, an American consulate worker, and her husband Arthur, and of Jorge Salcido, the husband of a U.S. consulate employee, and the murder of Robert Krentz, a rancher in Douglas, Arizona, underscored the cross-border nature of this problem.

I've supported the assignment of federally funded National Guardsmen to our southern border in the past and I have endorsed Arizona Governor Brewer's recent request for 250 federally funded National Guardsmen in Arizona to assist in this effort to stop the flow of illegal immigrants and narcotics.

I'd like to insert, Mr. Chairman, two letters into the record, one I wrote to Secretary Napolitano on March 29th and the other addressed to the mayor of Douglas, Arizona, on March 31st in this regard.

Chairman LEVIN. They will be made part of the record.

[The information referred to follows:]

Senator MCCAIN. Unfortunately, the administration has rejected Governor Brewer's request.

Admiral, I'm interested in your assessment of the security situation along the border and what steps can be taken to improve not only the ability of the United States to confront this drug trafficking threat, but also the ability of our allies in Mexico.

Admiral, I understand that yours is a military command and your role is one to be carried out in combat. I can make an argument that we are in combat with the drug cartels in Mexico. I can make an argument that the war between the drug cartels and the government of Mexico directly threatens the very existence of the government of Mexico. I don't say these words lightly, and I think that it's very clear that when you're talking about a $65 billion a year business that is harming American citizens and killing them because of the product, that this struggle with the drug cartels is going to and already has spilled over into the United States of America and has taken the lives of American citizens.

So I look forward to perhaps taking a visit with you to our southern border. I look forward to working with you and determining how we can best use some of the military equipment we have, such as surveillance technologies, use of UAVs, and better ways to enforce our border and make sure that it is secure. So I look forward to discussing this and working with you, Admiral Winnefeld. This is a grave threat and I am afraid that a lot of Americans are not aware how serious the consequences would be of the government of Mexico failing and being overthrown by these drug cartels, or at least marginalized so that the drug cartels can act freely, and the consequences to American security.

So I thank you and I will look forward to your testimony and look forward to working with you as we carry out what I believe is a national security requirement, and that is to secure our southern border.

I thank you, Mr. Chairman.

[The prepared statement of Senator McCain follows:]
[COMMITTEE INSERT]

Chairman LEVIN. Thank you very much.

General Alexander, you could have no more effective advocate than Senator Mikulski. I want you to know that this has been a long period of time for considerations because of the newness of this position and the importance that it has for the reasons which we've stated. But I don't think a week went by during this long period that Barbara Mikulski did not ask me: So when's the hearing? And you're lucky to have her as a Senator, but also as a wonderful advocate.

Senator MIKULSKI.

STATEMENT OF HON. BARBARA MIKULSKI, U.S. SENATOR FROM THE STATE OF MARYLAND

Senator MIKULSKI. Thank you very much, Senator Levin, Mr. Chairman, Ranking Member Senator McCain, and colleagues. I have the opportunity today to introduce Lieutenant General Keith Alexander, who is the current Director of the National Security Agency, located in Fort Mead, Maryland. I also am very proud to sit here today with also Admiral Winnefeld, and I would like to reecho really Senator McCain's sense of urgency about another war that we're fighting south of our own border.

I'm here today in my scope as the Senator from Maryland. My State is the home to the mother ship of signals intelligence in the U.S. military, which is the National Security Agency. And I would recommend in a classified hearing that the scope, breadth, and talented work force, the nature of it really be further explored, because I think it's often underestimated and it's undervalued because it does come in under everybody's radar.

But today is an exciting day in introducing General Alexander for his confirmation hearing to lead something called the Cyber Command. He will elaborate on that command, but I'm going to elaborate on General Alexander. President Obama nominated him and I think it's a great choice. This job, to head up the Cyber Command, is going to require expertise, leadership, and know-how. The know- how is going to require technical competence in fields that change in web years, not in fiscal years. It requires someone who has incredible organizational skills that could head up major dotcom companies in our own country and the diplomatic skills to navigate not only with foreign leaders, but the vagaries of our own governance structures.

I believe that General Alexander brings all of those talents and skills and even more. He brings a great deal of expertise. His biography speaks for itself and the command recognitions that he's received. He's been the head of NSA for 5 years. He was the Deputy Chief of Staff at the Army, General of the U.S. Army in Intelligence Security Command, and the Director of Intelligence for the U.S. Central Command, and numerous other positions.

That's kind of the resume stuff. But as you know, all of you here, that it is one thing to talk about credentials and bars on the shoulder and so on, but it's another thing to talk about leadership. I believe that General Alexander has led the transformation of the National Security Agency from an agency that was once focused on

Cold War threats to now a world of new world threats, supporting both people who are literally in battle in Iraq and Afghanistan, standing sentry over those others who have predatory intent against us, and bringing that leadership.

Right now he is leading the fight against cyber spies who want to steal our state secrets, cyber terrorists who want to disrupt everything from our financial services to our power grids, while supporting the wars in Iraq and Afghanistan, working with the Northern Command and our forces at the border protecting our borders.

So Lieutenant General Alexander is a leader and a professional. I believe he's an indispensable asset. He's had to deal with everything from other generals and admirals to deal with us and our often sluggish response to situations. He's had to deal with Google as it's been threatened by China and he's had to develop a work force and develop technology and he's had to do it with speed, diligence, while he's trying to avoid attacks on the United States, he's been trying to avoid fiscal boondoggles with his own agency.

The Cyber Command leader needs to be respected by the military. His service speaks for itself. He needs to be able to deal with the private sector. They're already coming to him for advice and how to work with us to protect dot-mil and other important things. And he's been a promoter of innovation.

I come to this because the community must come to deal, have a sense of urgency, not only on the confirmation, but on cyber security. Those who have predatory intent against us are dealing in web years. They're continually focusing on the rapidity of change in a dynamic web environment. That's every 3 months. We deal in fiscal years, Congressional sessions, quadrennial reviews. That's pretty dated when it comes to cyber security.

Our cyber shield is thinning. We need a unified response. We need a Cyber Command and we need the leader who's got the right stuff to do it. I believe that's General Alexander and I hope you confirm him with web year speed.

Mr. Chairman, I thank you for your kind attention.

[The prepared statement of Senator Mikulski follows:]

[COMMITTEE INSERT]

Chairman LEVIN. Thank you so much, Senator Mikulski. We haven't acted yet with web year speed, but we surely from this point on would hope to do so. The reasons we haven't are the reasons that I tried to outline, though, in my introduction, which set out, intended to set out at least, some of the very, very significant issues that this new command raises. But your eloquence is very, very helpful in this regard and your comments are very welcome.

Senator MIKULSKI. Good luck. I've got your back.

Chairman LEVIN. Admiral, I think we're going to start with you, so please proceed with your opening comments and please introduce anybody that you'd like to introduce to us. We always welcome family and friends should people be lucky enough to have them with them.

STATEMENT OF VADM JAMES A. WINNEFELD, JR., USN, NOMINATED TO BE ADMIRAL AND COMMANDER, UNITED STATES NORTHERN COMMAND/COMMANDER, NORTH AMERICAN AEROSPACE DEFENSE COMMAND

Admiral WINNEFELD. Yes, sir. Chairman Levin, Senator McCain, and distinguished members of this committee: It's a great honor to have been nominated by the President to become the Commander of U.S. Northern Command and the Commander of North American Aerospace Defense Command, and I thank you all for the opportunity to appear before you this morning.

I'm joined this morning—and thank you, sir—by my family and with your permission I'd like to introduce them: first my wonderful wife and best friend, to whom I owe so much, from Menomonie, Wisconsin, my wonderful wife Mary, who is a volunteer for the Navy and Marine Corps Relief Society here in Washington and who brings so much joy into my family's life. Sweetheart.

Here also are my two sons, of whom I'm so proud: my son LJ, who tells me he'd like to follow his father's footsteps into the Navy; and his brother Jonathan, who tells me he would prefer to serve in the Marine Corps.

Chairman LEVIN. Both of them belong in school. How come they're not there today?

[Laughter.]

Admiral WINNEFELD. I think they got a senatorial waiver, sir.

Mr. Chairman, over the last 3 years my friend General Gene Renuart has led the U.S. NORTHCOM and NORAD team with distinction and he'll leave behind a tremendous legacy of continuous improvement. If confirmed, I look forward to being able to build upon his efforts.

In this light, I'd like to make two simple but important points before receiving your questions. First, I can think of no greater responsibility than protecting our people and our way of life by leading our homeland's last military line of defense and by providing support at the Federal, State, and local level in times of great need. There are no points for second place in either one of these missions and I view this as a sacred trust.

Second, I have observed no other commands, no other combatant command for sure, in which cooperation with and support for partners is more important than with U.S. NORTHCOM and with NORAD. I believe the significant part of my career and my professional life spent in joint assignments has helped prepare me for this task.

So if confirmed, I will reinforce the critical importance of close partnerships and teamwork with the other combatant commanders and service chiefs, with the Department of Homeland Security, and a host of other inter- agency, State, local, and nongovernmental partners, with our close friends and neighbors Canada and Mexico, and with the National Guard and Reserve.

I view all of these relationships as vital, but I would like to particularly emphasize the latter. Our Nation's Guard and Reserve have never been better or more versatile and I look forward, if confirmed, to forging a strong personal partnership with them.

I also look forward to working closely with the members of this committee to ensure we're correctly tackling the critically impor-

tant job of defending our homeland and providing support to civil authorities.

Once again, I'm very grateful for the opportunity to appear today and I'd like to thank you, Mr. Chairman and Senator McCain, and the members and superb staff of this committee for the ongoing support that you provide to our men and women in uniform and to their families.

I look forward to your questions.

[The prepared statement of Admiral Winnefeld follows:]

Chairman LEVIN. Thank you so much, Admiral. We welcome you. We welcome your wife and your kids here today. We know how much you treasure them and we are delighted to see them here.

General ALEXANDER..

STATEMENT OF LTG KEITH B. ALEXANDER, USA, NOMINATED TO BE GENERAL AND DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE/COMMANDER, U.S. CYBER COMMAND

General ALEXANDER. Chairman Levin, Senator McCain, distinguished members of the committee: It is a distinct honor and privilege to appear before you today. I am honored that President Obama and Secretary Gates have placed their trust and confidence in me by nominating me for the position of Director, National Security Agency, Central Security Service, and for Commander, U.S. Cyber Command. If confirmed, I look forward to working closely with the committee to address the cyber security challenges facing our Nation today and in the future.

Sir, I'd like to introduce my wife Debby, who is with me today—right here, just so I can identify her. Debby has overseen 20 moves, experienced the highs and lows of almost 35 years in the service, brought 4 lovely daughters into the world, and is grandmother to our 12 grandchildren. I am indebted to her for her love, unflagging support, wise counsel, and occasionally letting me win in Yahtzee.

We face a growing array of cyber threats, from foreign intelligence services, terrorist, criminal groups, and individual hackers, who are capable of stealing, manipulating, or destroying information that could compromise our personal and national security. The Department of Defense in particular requires a focused approach to secure its own networks, given our military's dependence on them for command and control, logistics, and military operations.

In recognition of this, Secretary Gates directed the creation of U.S. Cyber Command to establish a framework under which a single military commander can achieve unity of command and operational integration across the full range of cyber space operations.

If confirmed, my main focus will be on building the capacity, the capability, and the critical partnerships required to secure our military's operational networks. This command is not about efforts to militarize cyber space. Rather, it is about safeguarding the integrity of our military's critical information systems. Working with U.S. Strategic Command and Department leadership and with help from this committee, my goal, if confirmed, will be to significantly improve the way we defend ourselves in this domain.

If confirmed, I also intend to draw upon the extensive lessons I have learned over the almost 5 years serving as both Director of

NSA and Commander of the joint functional Component Command Net Warfare, to ensure that Cyber Command can effectively leverage NSA's global intelligence capabilities.

I would like to note, however, that while there will be, by design, significant synergy between NSA and Cyber Command, each organization will have a separate and distinct mission with its own identity, authorities, and oversight mechanisms. NSA's own mission and authorities will not change as a result of the creation of this command and, while cyber space is a dynamic, rapidly evolving environment, what will never change will be an unwavering dedication by both Cyber Command and the National Security Agency to the protection of civil liberties and privacy of American citizens.

Finally, if confirmed, we can stand up the command under existing authorities, but there is undoubtedly much unchartered territory in the world of cyber policy, law and doctrine. If confirmed, I intend to work closely with the Under Secretary of Defense for Policy charged by Secretary Gates to develop a comprehensive strategy for DOD's cyber space operations. I will also rely heavily on the wisdom and guidance of this committee to ensure that we get this critically important mission right for our military and for our Nation.

In closing, I want to again express my sincere appreciation to this committee for holding today's hearing. If confirmed, I look forward to working closely with you. Your wisdom, support, and sustained engagement are critical to ensuring the success of this endeavor.

Thank you again for the opportunity to be here with you today. I look forward to your questions.

[The prepared statement of General Alexander follows:]

Chairman LEVIN. Thank you very much, General. We welcome you. We welcome your wife. I'm a little bit jealous of the 2 of you with four daughters—I only have 3—and 12 grandkids—I only have 5. But it's wonderful to have you both here.

I want to explore with you, General Alexander, some of that unexplored territory that you just mentioned, cyber policy, cyber law, cyber doctrine. You as the first Commander of Cyber Command are going to be in a critical position, not just in commanding the command, but in really setting the precedents for how that command is going to operate. There's a lot of unchartered territory, and you and I have talked about this.

What I'd like to do is share some hypothetical scenarios. You and I talked about your doing this and I wanted to let you know that that's what I wanted to do because I wanted you to be able to know in advance really what these scenarios are and to give us your thoughtful response to these. This is a new area, not just for our country, but an area which is particularly challenging, I must say, to me, being generationally challenged when it comes to understanding some of these issues.

So let me give you the hypotheticals, starting with the easiest one, I think, which is: Assume the following: That U.S. forces are engaged in a traditional military conflict with a country, we'll call it Country C. Now, how would you conduct cyber operations in that country in support of the combatant commander? Under what au-

thorities, processes, and orders would you be operating in that particular scenario? And then I'll give you two additional scenarios.

General ALEXANDER. Yes, sir. We would be operating under Title 10 authorities, under an execute order, supporting probably that regional combatant commander. The execute order would have the authorities that we need to operate within that country. We have standing rules of engagement of how to defend our networks.

I think that's the straightforward case. There would be an execute order that comes down to that regional combatant commander, that includes the authorities for cyber parsed and approved by the President.

Chairman LEVIN. All right, so that is kind of a traditional role. You've got an existing—an execute order. You've got rules of engagement.

By the way, we'll have an 8-minute first round.

Now the second hypothetical. I want to add a complicating factor to the scenario. Assume that an adversary launches an attack on our forces through computers that are located in a neutral country. That's what you've determined. The attack is coming from computers in a neutral country. How does that alter the way that you would operate and the authorities that you would operate under?

General ALEXANDER. Sir, that does complicate it. It would still be the regional combatant commander that we're supporting under Title 10 authorities. There would be an execute order. In that execute order and the standing rules of engagement, it talks about what we can do to defend our networks and where we can go and how we can block.

The issue becomes more complicated when on the table are facts such as we can't stop the attacks getting into our computers, and if we don't have the authorities in accordance with the standing rules of engagement we'd go back up to Strategic Command, to the Secretary and the President for additional capabilities to stop that.

But right now the authorities would be to block it in theater under the current standing rules of engagement, and it would be under an execute order, and again under Title 10 in support of that regional combatant command.

Chairman LEVIN. Is that execute order likely to have the authority to do more than defend the networks, or would you have to likely, in all likelihood, go back for that authority if it were more than defensive?

General ALEXANDER. Sir, it would probably have the authority to attack within the area of conflict against the other military that you're fighting. And there would be a rules of engagement that articulate what you can do offensively and what you can do defensively. And sir, in offense that's both in the exploitation and in the attack role. So both of those would be laid out in the execute order.

What you would not have the authority to do is to reach out into a neutral country and do an attack, and therein lies the complication from a neutral country: What do you do to take that second step?

Chairman LEVIN. And neutral being a third country, presumably? Is that synonymous or does the word "neutral" mean literally neutral?

General ALEXANDER. Well, it could be either, sir. It could be a third country or it could be one that we don't know. I should have brought in attribution, because it may or may not be a country that we could actually attribute to, and that further complicates this. And the neutral country could be used by yet a different country, the adversary, and it's only an attack through.

In physical space it's a little bit easier to see firing from a neutral country, and I think the law of armed conflict has some of that in it. It's much more difficult and this is much more complex when a cyber attack could bounce through a neutral country, and therein lies the complexity for this problem.

Chairman LEVIN. And that's the complexity that you've addressed.

Now a third scenario, more complicated yet. Assume you're in a peacetime setting now. All of a sudden we're hit with a major attack against the computers that manage the distribution of electric power in the United States. Now, the attacks appear to be coming from computers outside the United States, but they're being routed through computers that are owned by U.S. persons, located in the United States. So the routers are in here, in the United States.

Now, how would CYBERCOM respond to that situation and under what authorities?

General ALEXANDER. Sir, that brings in the real complexity of the problem that we face today, because there are many issues out there on the table that we can extend, many of which are not yet fully answered. Let me explain.

First, Department of Homeland Security would have the responsibility for the defense of that working with critical infrastructure. Department of Homeland Security could, through the defense support to civilian authorities, reach out to the Defense Department and ask support. Sir, one of our requirements in the unified command plan is to be prepared for that task. So we would have that responsibility.

If asked to do that, again we'd get an execute order and we'd have the standing rules of engagement that we operate under all the time. The issues now, though, are far more complex, because you have U.S. persons. Civil liberties, privacy all come into that equation, ensuring that privacy while you try to on the same network potentially take care of bad actors. A much more difficult problem.

As a consequence, you have a joint inter-agency task force, the Federal Bureau of Investigation, who has a great joint cyber investigative task force that would be brought in. All of these come to bear.

This is the hardest problem because you have attribution issues, you have the neutrality issues that we mentioned in the second scenario, you have inter-agencies working together with industry. I think that's one of the things that the administration is trying to address with Department of Homeland Security and with the Defense Department, how do we actually do that with industry? That's probably the most difficult and the one that we're going to spend the most time trying to work our way through: How does the Defense Department help Homeland Security in a crisis like that?

Chairman LEVIN. Is that policy that's now under way in terms of debate and discussion, is that scheduled for completion by the end of the year? Is that what the hope is, the goal is, for that?

General ALEXANDER. I think the Defense Department portions that would support that are, yes, sir.

Chairman LEVIN. Admiral, let me ask you about the missile defense system that we have. If I have time, I'll ask about the issue, the Ground-based Midcourse Defense System that we have in Alaska and California. But as I may run out of time, let me focus first on Europe.

We have a ballistic missile defense system in Europe. Last September the President announced a new missile defense plan for Europe that was unanimously recommended by Secretary Gates and the Joint Chiefs of Staff. That plan includes a number of elements that are intended to enhance the defense of the United States against potential future long-range Iranian missiles, particularly long-range Iranian missiles.

The forward-deployed radar in southeastern Europe would be part of that. Development of an improved version of the Standard Missile III Block 2 for deployment in Europe. This of course would work to complement or in concert with the Ground-based Midcourse defense system that I referred to.

But first, do you agree that that new missile defense plan will improve our capability to defend the homeland against potential future long-range missiles from Iran?

Admiral WINNEFELD. Senator, in particular the radar that would be placed presumably in southeastern Europe or in the southeastern part of that AOR would provide much earlier warning of a missile attack from Iran and therefore give much earlier warning for the ground-based missile or ground-based midcourse system in the U.S. to launch, and potentially that will dramatically raise the ability of that system to counter a threat coming from Iran. That's the most important part. The SM III Block 2, obviously further down the line with some potential ICBM capability is an adjunct to that.

Chairman LEVIN. And if the Russian radars finally were able to be joined to that system, would that add capability?

Admiral WINNEFELD. If the Russian radars are able to feed in into that system, then presumably, yes, sir, it would augment that capability on top of the radar that we would have in southeastern Europe.

Chairman LEVIN. Thank you very much.

Senator McCain.

Senator MCCAIN. Thank you, Mr. Chairman.

General Alexander, I think it would be helpful for this committee, and also I note the presence of the Chairman of the Homeland Security Committee, if perhaps you could submit to us for the record some of the changes that you think are needed both in law and in regulation to allow you to perform your functions in a not only more efficient fashion, but to make sure that you are protected constitutionally. Do you see my point, General?

General ALEXANDER. Yes, sir.

Senator MCCAIN. Do you think that would be helpful to the committee and the Congress, for us to sort of get a laundry list of what

you think needs to be done in order for you to be able to carry out your duties in a most efficient fashion, effective fashion?

General ALEXANDER. Yes, sir. We'll do that, sir.

[The information referred to follows:]

Senator MCCAIN. And perhaps working with, Mr. Chairman, the chairman of the Homeland Security Committee, we can try to—I think it's obvious from General Alexander's testimony close coordination between the Department of Homeland Security and the Department of Defense is obviously critical in maintaining effective—or taking effective measures in this new cyber war that we are in.

Admiral Winnefeld—

Chairman LEVIN. If I could just support what your request is on that, Senator McCain. It's a very useful point and the answer that you give to us in response to Senator McCain will go to the Homeland Security Committee as well. It's a very important point. Thank you.

Senator MCCAIN. It may at some point argue for a joint committee hearing, depending on how urgent the needs are. But this is obviously a brand new field of combat and one that we are going to have to make significant adjustments to.

Admiral Winnefeld, you are new in your responsibilities and I congratulate you for your long years of service. Do you agree with my opening statement concerning this real crisis we have on our southern border and with our southern neighbor concerning this struggle, the existential struggle of the government of Mexico with the drug cartels?

Admiral WINNEFELD. Senator, I certainly share your deep concern over the levels of violence in Mexico and along our border and certainly the corrosive effect that it ultimately has inside our cities.

Senator MCCAIN. Have you had time yet to assess whether the government of Mexico—and we are helping out a great deal. I think it's $1.5 billion in the Merida Plan. Have you any assessment as to whether we are succeeding or failing or where the drug cartels are as far as this struggle is concerned? Have you an assessment of the situation yet?

Admiral WINNEFELD. Senator, I'm in a early stages of my assessment, to be quite honest with you. In preparation for the hearing, I've done my own reading. I was privileged to accompany the large delegation that the government sent down to Mexico City in March to meet with their counterparts in Mexico, and I'm watching this very closely. Of course, if I'm confirmed I intend to really burrow into it once I get out and in command.

Senator MCCAIN. Would you agree that your initial assessment is that the government of Mexico is in an existential struggle with the drug cartels?

Admiral WINNEFELD. I believe that the drug cartels really want to be left alone. They want to have space for them to compete for market share. I don't believe at this point that they are intent on overthrowing the government of Mexico. However—

Senator MCCAIN. No, I agree with that assessment. But if the government does not have control of large parts of its territory, then, if not an existential threat, certainly a threat to its ability to govern.

Admiral WINNEFELD. Yes, sir.

Senator MCCAIN. Have you had an opportunity yet to visit the border?

Admiral WINNEFELD. I have not, and I was delighted that you made the offer during your opening remarks, sir, because it's one of my very first priorities, if confirmed. When I get out there, I want to get down there and see for myself what's going on. I would very much welcome the opportunity to accompany you on a trip down there, sir.

Senator MCCAIN. I would look forward to it, and soon, Admiral.

One of the aspects of this struggle we're in—and I'm very aware of our Constitution and the role of the military inside the United States and all of that. But I also would argue that when we have a level of violence that thousands of people are being murdered on the other side of the border, American citizens have been murdered, as I just described to you, that at least we ought to look more, scrutinize more carefully and utilize some of the lessons we have learned in, say, in Iraq. And I mean—what I mean by that is surveillance capability as well as physical barriers.

I do not mean to draw too close a comparison between the war in Iraq and our struggle on the border. But I do believe you could make a comparison between the use of, say, UAVs, surveillance capabilities, as well as barriers. We all know that barriers only work if they are surveiled and maintained. It seems to me that we could use some of the technology that we've developed in Iraq and are using in Iraq and Afghanistan to better surveil and enforce our borders, because I'm not sure when this struggle between the Mexican government and the drug cartels is going to be over, but I do believe it's going to be a while, and I do believe that therefore we have the obligation to secure our borders to prevent further incidents such as the murder of a rancher in Douglas, Arizona, just a short time ago.

So I look forward to visiting with you on the border. Every area of the border has its challenges. I think factually that the Tucson border area has the largest number of incursions. We also have the Goldwater Ranges, as you know, down near the border and that—some of the illegal activity has affected our training capabilities there. So there's a number of implications associated with the struggle on the border that argues I think for our highest attention.

I hope that you would also, as we assess this situation, would help us assess the manpower requirements as well as the technology requirements, since our governors in the border States have said that they need the National Guard there. That response has not been made, met with—that request has not been met with a favorable response as yet.

So I would look forward to it and will go to work right away. Frankly, I am more concerned than I have ever been about the fact that many indicators are that the drug cartels are certainly not losing, if they're not winning. And if they're not losing, as you know, in any war, then they are winning. This is an irregular warfare kind of situation. It has many different complications. Where are they getting the sophisticated weapons? The Mexican police and army many times are outgunned. Also, this effect on the United

States of America of what is judged to be about a $65 billion a year business as well.

So I thank you for your commitment to get down there and I look forward to joining you as soon as possible. I know that my colleagues that represent border States share the same concern that I do about the size and implications of this issue.

I've been down there many, many times over the years and I've visited Mexico City. I have the greatest respect and admiration, and I know you do because you were in Mexico City for President Calderon. I think he is doing everything that they can, but I think they are crippled by corruption and I think they're crippled by a lack of training and capability of their police and military.

But I also believe that we have made some very wise investments in helping them with technology and training that may be of significant benefit to them in the long run.

Do you agree?

Admiral WINNEFELD. Absolutely, sir, and I absolutely share your view that the Calderon government has exhibited extremely good leadership and courage in this fight, because one thing—if they wanted to immediately tamp down the violence, they could back off the pressure on the drug cartels, and they have had the courage to not do that. So I think it's a tremendous sign of our partner in Mexico, and I'm proud to have potentially the opportunity to work with them, yes, sir.

Senator MCCAIN. Thank you very much.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator McCain.

Before I call on Senator Lieberman, let me ask you the standard questions which we place before all of our witnesses, nominees. Have you adhered to applicable laws and regulations governing conflicts of interest?

General ALEXANDER. Yes, sir.

Admiral WINNEFELD. 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 WINNEFELD. No, sir.

General ALEXANDER. No, sir.

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

Admiral WINNEFELD. Yes, sir.

General ALEXANDER. Yes, sir.

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

General ALEXANDER. Yes, sir.

Admiral WINNEFELD. Yes, sir.

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

Admiral WINNEFELD. Yes, sir.

General ALEXANDER. Yes, sir.

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

General ALEXANDER. Yes, sir.

Admiral WINNEFELD. Do you agree, if confirmed, to appear and testify upon request before this committee?

General ALEXANDER. Yes, sir.

Admiral WINNEFELD. Yes, sir.

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

Admiral WINNEFELD. Yes, sir.

General ALEXANDER. Yes, sir.

Chairman LEVIN. Thank you very much.

Senator Lieberman.

Senator LIEBERMAN. Thanks, Mr. Chairman.

General Alexander, Admiral Winnefeld, thank you for your service to our country. I must say, going over your biographies in preparation for the hearing, your answers, listening to you this morning, you're two extraordinarily capable people and our Nation is fortunate indeed to have you in our service. I look forward to supporting your nominations.

General Alexander, I want to pick up a bit on the line of questioning that Senator McCain began. But first, just if you would briefly lay on the record, how as we stand up this new Cyber Command and you as its first leader, how serious is the cyber threat to the United States today? And to the extent that you're able to say in open testimony, particularly about the Department of Defense web sites and networks, how frequently are we today under attack?

General ALEXANDER. Sir, I think one of the underlying principles, beliefs, that the Secretary had for standing up this command was just the amount of attacks that we're seeing coming into the Defense Department gateways every day.

Senator LIEBERMAN. Right.

General ALEXANDER. Hundreds of thousands of probes a day.

Senator LIEBERMAN. Every day?

General ALEXANDER. Every day.

Senator LIEBERMAN. Right.

General ALEXANDER. The issue that we saw was how do you fight against that? And by putting the command together, I think that was the first, what he saw as the first big step that we need to make to build the capacity and to take that on. So we saw it as very serious. We have been alarmed by the increase, especially this year, both in the critical infrastructure within the Nation and within the Defense Department. So it's growing rapidly.

Senator LIEBERMAN. Right. So hundreds of thousands of probes, these are not attacks in the sense that we normally consider an attack; is that correct?

General ALEXANDER. That's correct, Senator.

Senator LIEBERMAN. They're an attempt to probe and to exploit our system to gain information?

General ALEXANDER. That's correct, Senator. They may scan the network to see what type of operating system you have, to then facilitate an exploit or an attack.

Senator LIEBERMAN. Right. And is it fair to presume that, while some degree of these are individual hackers, others are working for nation states that are trying to determine what they can about our defense structure?

General ALEXANDER. That's correct, Senator.

Senator LIEBERMAN. Okay. That I think quickly but strongly outlines the nature of the threat certainly to our National security structure.

Let me get into some of the questions about the relationship between the Department of Defense and the Department of Homeland Security because, as Senator McCain said, I'm privileged to be chair of the Homeland Security Committee. There's a lot of overlap, not surprisingly, between the membership on these two committees.

The existing system allocates responsibility between the Department of Defense and Homeland Security, the Department of Defense obviously having responsibility not only for offensive cyber operations, but for the defense of the Department of Defense's networks. The Department of Homeland Security has responsibility for defending the civilian networks of our government and working with the private sector to defend the civilian infrastructure, which probably itself would be a target of attack, could be certainly at some point.

I welcome Senator McCain's suggestion that these two committees work together and that we have your responses to how we might clarify responsibilities in the future. But I think it is important to get on the record the extent to which NSA, which you head, is now cooperating with the Department of Homeland Security in enabling its work. The bottom line here is that NSA is a treasure, a national treasure. Its resources are extensive. No one I think would want the Department of Homeland Security to try to replicate those resources to carry out its responsibility to protect Federal Government civilian networks—and civilian networks.

So I wanted to ask you—and therefore the cooperation is really critically important. Can you explain both what that relationship is now and how you envision Cyber Command that you'll now head and NSA playing a supporting role to the Department of Homeland Security in protecting non-military networks?

General ALEXANDER. Senator, I'm going to break that into two parts, one that talks about what the National Security Agency is doing to support Department of Homeland Security in executing their mission. As you stated, it's their mission to defend the rest of the dot-gov and to work with the civilian community for critical infrastructure. Our responsibility is to provide technical support to the Department of Homeland Security. We do that under the critical—the comprehensive national cyber initiative—to help them build the technology that they need to defend those networks.

In part of that, sir, we have a responsibility to provide them the technical information for what the threat is trying to do to them.

Senator LIEBERMAN. Right, right.

General ALEXANDER. Provide them early warning to that. But they would operate and defend that system. So our responsibility, we provide people and capabilities to help them do that.

I think that partnership continues to grow. We've had a number of meetings and I think we're trying to work through it. That's parts of the issue, as you can see. So then I think what Secretary Napolitano and the country's going to have to look at, how do we work with private industry, who owns and operates many of these networks?

Senator LIEBERMAN. Right.

General ALEXANDER. On the Cyber Command side, if a crisis were to occur, now Cyber Command or the Defense Department may be called in to help, defense support to civilian authorities. What we would be asked to do is dependent on the situation. It could go through Northern Command, it could go to STRATCOM or to Cyber Command the provide either technical support or help prevent an attack, or in the case of a sustained attack actually prevent—help defend our networks.

So those are the cases, and as you get into each one of those you run into a series of issues that we have yet to work out with the roles and responsibilities, especially with private industry.

Senator LIEBERMAN. Right. That was very helpful.

The second situation, the second area of overlap, would be in what I would describe as a national security crisis, the extent to which Cyber Command would come in and work with the Department of Homeland Security to defend either Federal Government civilian networks or private civilian networks; is that correct?

General ALEXANDER. That is a mission that we would plan for under the unified command plan and that we have to work out the specifics of how to do that.

Senator LIEBERMAN. Am I correct that you would say that the current allocation of responsibility between DOD, Cyber Command, NSA, and the Department of Homeland Security is a good one? Understanding that you've got to work out some of the questions you've talked about, but bottom line, that DOD has responsibility for the defense networks in Defense and DHS has responsibility for the Federal Government civilian networks and private civilian networks?

General ALEXANDER. Yes, sir. I think it is absolutely important to have DHS operate and defend those networks. I also believe that there necessarily needs to be a linkage and leverage of that capability for us to provide the technical support, the early warning, and others. I think we're walking down that road. I think it is written out right, but there's more to understand as we go into that, what are the exact lanes in the road for that and how can we help, and what happens in a true crisis.

Senator LIEBERMAN. I appreciate that answer very much.

One of the things I think was implicit in what Senator McCain said, and I certainly share this hope, is that we can work together to determine both with yourself and Secretary Napolitano whether there are any legislative changes necessary to enable Department of Defense components to better assist the Department of Homeland Security in its cyber security mission.

General ALEXANDER. Yes, sir.

Senator LIEBERMAN. Thank you.

Thanks, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Lieberman, and we will work closely as committee chairmen, and our ranking members I know will be joining us in this coordinated effort—

Senator LIEBERMAN. Good.

Chairman LEVIN.—to understand this new world and to oversee it properly.

Senator LIEBERMAN. Thank you.

Chairman LEVIN. Thank you very much.

Senator Inhofe.

Senator INHOFE. Thank you, Mr. Chairman.

I only wish I knew as much about this as Senator Lieberman does and Senator McCain, because I'm kind of new to this and when I saw your command, as I told you when you were in my office, surface, I started getting into it and recognizing that there is a reason for it, and that there are problems out there.

Chairman LEVIN. Senator Inhofe, if I could interrupt just for a moment. I'm going to have to leave for a short time and I've asked Senator Udall, who will be next in line anyway to ask questions, if he could then continue after that. He indicated he could. So after you're completed, Senator Inhofe, it'll go then to Senator Udall, then back to somebody on your side if there is someone here. But Senator Udall can take care of that.

Thank you.

Senator INHOFE. Yes. Over the last decade as the use and connectivity has become more pervasive, most of the IT security spending has been invested in perimeter defense of the distributed network. There has been a reduction in appropriations or in spending in some of these areas, and I am concerned about that.

I've been told that the DOD has created and adhered to a strict set of security configuration controls for their mainframe systems, but there have been some reports of classified government systems being breached. I'd like to have you just take as much time and as much detail on this, the problems that we have.

Then second, I want to talk about some of the civilian—some of the systems outside of the military that I'll be asking you about, due to something that appeared this morning in the media. But does the DOD have any issues with its mainframe security, both in its air- gapped or non-wired systems and in the systems that are connected to the Internet? What problems do you see that you haven't already mentioned in the previous questions?

Again, I apologize for not being here for your opening statement, so you may have covered this. If so, that's fine.

General ALEXANDER. Yes, sir. I think the key issue that you bring up is some of the legacy defense capabilities would look at a perimeter defense. As we begin to merge our offense and defensive capabilities onto one team, one of the things we did was change the strategy from perimeter defense to defense I depth.

Senator INHOFE. Okay. Now, before that took place—and I'm sorry I have to ask this question; I should know and I don't—who was doing this then?

General ALEXANDER. Well, this was separated in responsibilities between what the network defenders and operators would do versus what you would do in the attack and exploit arena.

Senator INHOFE. Okay.

General ALEXANDER. In many of our war games, in many of our exercises, we noted that the offense always had the upper hand. When you look at that, the red teams and the blue teams that we would bring out to test our networks we saw were largely successful. As a consequence, one of the issues that we said is can we bring some of that great talent that's on the offense to help on the defense? When we started doing that, we made changes to some of our doctrine, some of the operational concepts, and some of the ways that we do it.

You bring out a key one, Senator. That is defense in depth. That's absolutely important because the adversary is always going to try to penetrate our network. We have to remain vigilant and try new capabilities, tests, and always be on the Guard for those exploits or attacks into our network.

Senator INHOFE. That's good and I appreciate that.

This morning on the—it's called "Dark Reading"; it's a business IT, information technology, web site—they talk about, even with minimal Internet access, malware and breaches are increasingly occurring. Utility processing—now we're talking about the non-military, non-defense field. While only 10 percent of the industrial control systems are actually connected to the Internet, these systems that run water, waste water, utility power plants have suffered an increase in cyber security incidents over the past 5 years.

Now, why don't we shift over into what is being done to secure those networks and systems that are not government or military, but are critical to us, such as those that are mentioned in this article? What are you—what do you anticipate to do—you've talked about the problems that are out there—in terms of approaching those problems, finding solutions? And then getting into the technology, do you really have the resources that you need to do what you think, you anticipate, you're going to have to do in these non-military, non-defense areas?

General ALEXANDER. Sir, the key issues that come on the table as you lay that out is most of our infrastructure for our government is owned and operated by private industry. If we are going to be successful in defending our networks, we have to have a great partnership between Department of Homeland Security, who has the lead in this area with civilian industry, with the Defense Department and intel community to bring in those techniques and the early warning to work with private industry. That's the hard issue that I see facing us today.

Senator INHOFE. What I would ask you is, as this progresses, I'm very interested in this. As I mentioned in my office, if we could keep an ongoing conversation as to what might be out there, what resources you might need, and so forth, because I see this as just a huge area. And you're the right person for it. I'm just glad that you're doing what you're doing. So I think that will probably take care of it.

Admiral Winnefeld, when you were in my office we talked about one of the major concerns I had. I was very much involved early on in the negotiations with both Poland and the Czech Republic on the radar site and on the third site that we were going to put in Poland. It was pretty risky on their part to do something that Russia was opposed to, and they agreed to do it. I was very much con-

cerned when that was pulled out from under them a year ago in the first budget of this administration.

Now, so I had two concerns. One was can they really believe what we're telling them? I've talked to them since that time and I think that's probably all right. But the whole reason for that is that, we all know that we have ground-based interceptors in Alaska and California and we know that we're in pretty good shape on anything coming from that direction.

My concern is this. Our intelligence tells us—and it's not even classified—that as early as 2015 they could have the capability in Iran of sending one over to the eastern part of the United States. Now, that may not be right. Maybe after that. But nonetheless it says it could be that early.

My understanding on the third site, that would be deployable by around 2012. I was very comfortable with that time. I know the arguments, and I heard you respond to Senator McCain's question. To me, if we're not going to use that third site or a site someplace else—at one time we talked about Florida—before the SM III 2–Bravo would be there—first of all, do you have any date at all that that would come into play, that that would be—where that could be deployed?

Admiral WINNEFELD. The SM III 2–Bravo is still under development.

Senator INHOFE. I know that.

Admiral WINNEFELD. And about 2020 I believe is when it would—

Senator INHOFE. That's the date that I have heard. What bothers me is what happens between 2015 and 2020? And I heard your response to that, but there has to be a percentage that's tied to that, because when we look at it—I've had a lot of briefings and I've seen the map of the coverage and the area of how far can they reach with both radar and interception capability from the West Coast to the East Coast. And frankly, I'm just not comfortable with that.

I'd like to have all the assurance I can have that what we're doing right now is not going to give us the vulnerability that I think we're going to have in that period of time somewhere between 2015 and 2020.

Do you want to elaborate on that?

Admiral WINNEFELD. Well, I would say that under the current laydown, Alaska and Vandenberg, that there is a footprint that covers the entire United States from both Iran and Korea. The percentages go up as you get the radar into Europe, and certainly if the SM III Block 2–Bravo pans out then they will go up accordingly.

I understand your concern completely about the potential risk in that little band before the SM III 2- Bravo would be on line, and if confirmed that's certainly something that I would want to understand better.

Senator INHOFE. Well, my time has expired, but I just would—when you say the percentages will go up, that's something you can't talk about in an open meeting. But maybe some time we'll have a chance to visit about that. Just keep me informed as this moves along because I do have a great concern.

Admiral WINNEFELD. I will, sir.

Senator INHOFE. Thank you.

Senator UDALL [presiding]. Thank you, Senator Inhofe.

I want to recognize Senator Reed for a minute. He has a special acknowledgment he wants to make.

Senator REED. Very briefly, I want to welcome General Alexander. I think we met about 40 years ago and in the intervening 40 years he has acquitted himself magnificently as a soldier. I'm very confident that your leadership will improve our National security.

Admiral, thank you for your service to the Navy, and to your family, and to Keith's family, too. But I'm sure we'll have a chance in the days ahead to talk seriously about these very critical issues. But thank you.

Thank you very much.

Senator UDALL. Thank you, Senator Reed.

Let me recognize myself for 7 minutes, and let's start with Admiral Winnefeld. Welcome. General Alexander also, thank you for taking the time to come by and see me in the last couple of weeks.

General Renuart was here recently and he talked about the synergy of his commands, Admiral, and what he believes is truly an interdependent relationship between NORAD and U.S. NORTHCOM. Can you tel us your thoughts about the relationship between NORAD and NORTHCOM?

Admiral WINNEFELD. Very close, clearly. The missions are very symmetrical, aerospace warning, aerospace control, and maritime warning for NORAD and of course homeland defense and defense support to civil authorities to NORTHCOM. So when you look at the fact that NORAD might be providing some aerospace warning of, for instance, the ballistic missile threat, that then NORAD would then assume the responsibility for defending against, then there's clear synergy there.

I think it's important and a good move that General Renuart has brought the staffs together. I know that the staffs enjoy that, and my understanding is that Canada shares that view. I think I look forward, if confirmed, to going out there and exploring it further.

Senator UDALL. We of course are looking forward to having you based in Colorado, and I look forward to working with you, as I have with General Renuart.

General Alexander, let me turn to you if I might. We talked about the benefits of dual hatting speaking of dual hatting in another setting, Cyber Command and NSA. You talked about your understanding of the importance that oversight transparency will play in this new structure. Yet in the advance questions you were only able to provide classified answers to what seemed to be some of the fundamental challenges facing Cyber Command. Is there anything you can tell us in this open session to get at some of those basic questions?

General ALEXANDER. I think first transparency is important, especially in the cyber arena, what we do on the National Security Agency side to support that and what we do on the Cyber Command side. The reason I say that, I believe that the government combined, Congress and the administration, to the American people, we've got to help explain that. We have to show what we're doing to ensure that we comply with the laws. As you may know,

Senator, we stood up a Directorate of Compliance at NSA to ensure that we train our folks significantly, we hold them accountable to complying with that. It is important to us, and we'll carry that into Cyber Command as well to ensure that we have those same things.

So it seems to me that that's one of the fundamental issues, that we all take an oath to the Constitution and that we support that Constitution. Our folks take that very seriously.

Senator UDALL. Let me follow on and turn the question to the relationship with Cyber Command and Northern Command. I'll ask you first to give us your thoughts and then I'll turn to the Admiral to provide his thoughts, if I might.

General ALEXANDER. I think there's a great partnership. We have already talked about this and our partnership would really go through requests from the Department of Homeland Security when they have an issue. From my perspective, I could be supporting or supported depending on the situation, and the Secretary would choose that. But it will be a close working relationship, and I think one of the key things that we'll look at in the future is asymmetric attacks in cyber space on this country and how do we help the Department of Homeland Security do their mission.

Senator UDALL. Admiral, would you care to comment?

Admiral WINNEFELD. Well, Senator, I've forged a close friendship with Keith Alexander over the last 18 months in our respective roles and we get along very well. I would first tell you that I look forward to being a satisfied customer if I'm confirmed in terms of having networks protected and potentially, if it came down to it, getting the types of information that I would need in order to perform my job as the Commander of NORTHCOM or NORAD.

I also believe that with the tremendous number of inter-agency relationships that a command like NORTHCOM has to have, that I'll have a tremendous source of information for General Alexander on the kinds of support that those people need, and of course with Department of Homeland Security in the lead. But he will be an integral player in that process. So I look forward to plugging into that system and helping in any way I can.

Senator UDALL. I understand when there's additional time available we can discuss the respective merits of the football teams at the two academies; is that accurate? Neither one of you need to—well, you look like you want to comment.

Admiral WINNEFELD. Well, being a graduate of the Georgia Institute of Technology, but being a very loyal Navy football fan, I think that we're in pretty good shape.

Senator UDALL. Let me leave that there.

General Alexander, at a recent conference the White House Cyber Security Adviser Howard Schmidt questioned whether an event such as a cyber war can exist, and I'll quote what he had to say. He said: "A cyber war is just something that we can't define. I don't even know how a cyber war would benefit anybody. Everybody would lose. There's no win-lose in the cyber realm today. It affects everybody. It affects businesses. It affects government. So, number one, there's no value in having one." End of his quote.

That leaves me, that statement, with a number of questions. Do you think that a cyber war can exist? Can you define it? If there's

no value in having one, is there a need for the U.S. to develop offensive cyber war capabilities?

General ALEXANDER. Senator, in general terms I do think a cyber war could exist. I believe it would not exist in and of itself, but as part of a larger military campaign. I believe that the tools and stuff for command and control that we have today to affect those in cyber space are analogous to the tools that we had 40 years ago for jamming communications. But now in cyber space you can not only jam, but you can do a lot more to information, and therein lies part of the problem.

We see that go on in civilian industry and governments around the world, public knowledge. So the issue is from a military perspective, if these things are impacting our networks today we have a responsibility the defend those and set up cyber security.

I think the steps that we're talking with U.S. Cyber Command is to do just that: How do we secure these networks and how do we bring those pieces of the team together under one single commander to benefit each of the combatant commands in our Nation as a whole?

Senator UDALL. The old doctrine—and it's still in some cases a very effective doctrine—of mutually assured destruction or deterrence certainly could perhaps apply in a cyber war or cyber context when you have nation states. But when you have a lot of these individual actors under way, they may not comport with existing both written and unwritten rules as to how you conduct these kinds of operations. Is that a fair characterization of the threat we face?

General ALEXANDER. Senator, it is. Attribution will be very difficult.

Senator UDALL. We can certainly track, for example, if a nuclear weapon is used the perpetrator of that particular attack, from everything I know. There are signatures tied to nuclear materials. But this is a much more difficult realm in which to understand who may have attacked us or tried to penetrate our systems; is that right?

General ALEXANDER. That's correct, Senator.

Senator UDALL. Let me move to this term "geek-speak" which I just became familiar with. You mentioned that in developing policies for how far Cyber Command can help protect critical infrastructure that trying to translate that into an understanding in the private sector is crucial. How are you going to convey the seriousness of the threats that now are framed in this geek-speak way, but the average individual or even the CEO in some of these civilian operations may not fully understand?

General ALEXANDER. Senator, I think our CEOs of many of the information technology companies are seeing the threats today and that's becoming increasingly more public knowledge. The banking community, your IT infrastructure, your antivirus community, I think they see. They're on the leading edge.

They have great capability, they have great talent. Therein lies parts of the issue, is the government's going to have to leverage part of that talent, because they own the infrastructure that the government operates on, and for continuity of government Department of Homeland Security has a tough set of issues. In crisis,

that's where calling between the Department of Homeland Security and the Defense Department, that's where the real issue is going to go.

I do think this is an education process, though. We're going to have to teach people several things: What are the rules and how are we operating? We have to be transparent in how we do it. I think that's one of the key things, so that they can see that what we're doing is just try to protect our networks, not invade their civil liberties and privacy.

That's a very difficult issue, because this area is so complex it's hard for people to see it. We've got to help them understand that. I think the way to do that is by showing you and other members of the committee and the government and critical infrastructure in Department of Homeland Security, a team, how we're doing it and ensure that that follows the right legal framework, that we're complying with that, and you can see how we actually audit ourselves and do that.

Senator UDALL. My sense, as I close, is that in order of focus and understanding, we're best prepared right now on the dot-mil domain, dot-gov next. But then when you get into the dot-com, dot-org, dot-edu, those are more vulnerable systems and networks.

General ALEXANDER. They have a wider spread, Senator, so some of them really are where you say, and some of them may be amongst the best. Your IT industry and antivirus are probably up at the top and others like you said, yes, sir.

Senator UDALL. Thank you. I look forward to working with both of you when you're confirmed.

Let me recognize the Senator from North Carolina, Senator Hagan.

Senator HAGAN. Thank you, Senator Udall.

I too want to thank both of you for your service in the past and certainly for your upcoming service in these new positions. I wanted to, Admiral Winnefeld, I want to be sure that your boys know that I think a Senate waiver in missing school today is critical. I think it's very important for them to be here. The rest of your families I think, family support, certainly allows you to do a much, much, much better job. So thank you to all of the families.

I also wanted to say I thought Senator Mikulski's introduction was right on. So we always enjoy hearing Senator Mikulski.

But Admiral Winnefeld, may defense analysts have noted that it's time for the Nation to look beyond the Goldwater- Nichols and institute reforms that will address the needs of a new strategic era in a manner that more effectively leverages all of the instruments of national power. As Commander of United States Northern Command, do you feel that there are any changes in organizational design or statutory authority that would enable you to more effectively close the seams between the DOD and the Department of Homeland Security and other governmental agencies with respect to creating a more integrated approach to homeland defense?

Admiral WINNEFELD. Senator, I think that the relationship between NORTHCOM and the Department of Homeland Security is illustrative in this regard. My understanding from what I've learned over the last couple of months here is that they do have a very close relationship, a very close working relationship, both at

the planning and exercise and training and operational execution levels.

At the planning levels, a lot of collaboration is going on, prescripted mission assignments that the Department of Homeland Security has worked out with NORTHCOM, and I can go on on the planning side. On the exercise side, the National exercise programs are participated in by both organizations. Then on the operational side, on a day to day operations piece, both of the command centers are connected together very, very well. There are liaison officers from each—from the Department of Homeland Security and into NORTHCOM, and vice versa.

Then of course, in the event of a disaster or some sort of event that would require NORTHCOM to support DHS, NORTHCOM very clearly I believe understands its supporting role.

So I think that relationship is very strong, but we are always receptive to new and better ways of doing business, to include all of the numerous partners that are involved in homeland security and homeland defense.

Senator HAGAN. So from the standpoint of statutory authority, you don't see a need for a change?

Admiral WINNEFELD. I don't think right now, Senator, we need any. But I will certainly keep an open mind on that, and I'm always willing to explore it.

Senator HAGAN. The U.S. armed forces responded to the devastating earthquake that struck Haiti in a tremendous fashion and we all want to give credit where credit is due. I think our military did great. The service members provided support to the relief effort that included assistance with the preservation of order, protection for vital supplies, and the overhead imagery of the devastated areas. I was able several weeks ago to shake 200 young men's hands as they were coming back from Haiti and just thank them for their hard work.

But Admiral Winnefeld, in the event that an equally devastating earthquake or hurricane were to strike here in the U.S., do you believe that you would have statutory authority to provide the same support to civil authorities which is essential to restoring public order in the aftermath of a natural disaster?

Admiral WINNEFELD. Senator, I believe that the events in Haiti were very instructive for us, for one thing. It was a very nearby reminder of the kinds of things that we're going to have to do in a disaster like that, heaven forbid that it happen inside our own country.

I do believe that most of the authorities that are required are there. I think there are a couple of additional things, at least one, that we need to pursue. As you're probably aware, we are interested in having the authority for the Reserve component to be activated in order to support the immediate support to the disaster there. I think that we've got a very good understanding with the governors and the National Guard on that and I think we can come to closure on that.

Senator HAGAN. Speaking of the National Guard, during Tuesday's Air-Land Subcommittee hearing I voiced concerns over the Air Force decision to transfer 12 C–130 aircraft from various Air National Guard units to an Air Force Reserve unit based in Arkan-

sas without consulting the affected adjutant generals or State governors. Obviously, North Carolina is one of the States where this is being discussed.

But within the total force structure, how do you intend to satisfy your statutory responsibilities for providing homeland defense and support to civil authorities at the Federal level without disrupting the capacity of State governments to do the same?

Admiral WINNEFELD. I think we have to have a very close partnership with the governors and with their adjutant generals, and if confirmed it's one of my very highest priorities, to develop that relationship, my personal relationship with the TAGs, to ensure that we have a very clear understanding and that they know that I'm a believer in supporting, playing the supporting role that NORTHCOM has been identified statutorily with in a crisis.

It's one of the things, if I'm confirmed, that I look forward the most to, is building that relationship.

Senator HAGAN. I think a lot of the individuals within those States are quite concerned about this request.

General Alexander, our growing reliance upon technologies, such as robotics, unmanned sensors, computer- based communications systems, has created a vulnerability within the architecture of our armed forces and within our government as a whole. Protecting the platforms and the networks that our Nation relies upon obviously must be treated as a priority, which is why I truly support the concept of a U.S. Cyber Command. I think we had a good discussion in my office this week about some of the areas of expertise that you bring to the table, as well as your concerns about many of the issues that I know that you'll be facing.

But as Director of the National Security Agency, Chief of Central Security Service, and Commander of U.S. Cyber Command, how do you envision leveraging the capabilities of each of these organizations in order to enhance our National security posture?

General ALEXANDER. Senator, perhaps one of the greatest honors I've had is to lead the National Security Agency. They have great people, tremendous people. Our Nation has put a lot into building the National Security Agency up—over 700 Ph.D.'s up there that have operated in this arena. We built this over 60 years. Billions and billions of dollars have gone into it.

Over the last 5 years we've had the privilege of having the joint functional component command net warfare and NSA together, so we could leverage that infrastructure and that talent. What I think this does for the U.S. Cyber Command is it puts our soldiers, sailors, airmen, and marines, the young folks that are coming in, with this experienced group for training, and when we deploy these folks forward to support regional combatant commands we have folks that know the best in the world that they can reach out—they operate at the tactical operational level and can talk to the strategic level, because in cyber space it's one network and we have to operate as one team.

So I think that absolutely one of the key principles is leveraging that human capital that we have within NSA that is absolutely superb, to help train, coach, and work with these in peacetime, crisis, and war.

Senator HAGAN. When you mentioned the 700 Ph.D.'s that are working there, I'm curious, and I know we talked about this, too, the human capital. I just left an Education Subcommittee meeting where we were talking about the reauthorization of the No Child Left Behind, and obviously we have to have an emphasis in education to be sure that you have the talented work pool that you need in order to conduct the requirements that are put before you.

Can you discuss a little bit about the quality of the work force that you're seeing and where you're recruiting individuals? If there something from an education standpoint that we need to do as a country, I'd be very curious as to your thoughts on that?

General ALEXANDER. Senator, I'm a huge advocate of STEM, science, technology, engineering, mathematics. I think it's absolutely crucial for our country that we continue to push our younger folks that way. We'll work on Admiral Winnefeld's great two sons here. It's the future for our country, having this.

We have some great—we have tremendous, great programs out there. I have personally seen what the Bill Gates Foundation is doing and how that's going throughout the country. What that does for us is build the capacity, the capability that we need, not just for U.S. Cyber Command and NSA, but for our country's leadership in this key area. That's absolutely important.

We have partnerships from our information assurance part with over 100 universities around the United States to help come up with curriculums that meet a certain set of standards that Department of Homeland Security and NSA jointly work. It is superb because it trains people on how to secure networks, what are the key fundamentals. They don't all come to NSA. Many of those will go out to industry and that's good for our country. But we do get an awful lot of good talent.

What I would say is we've got great people, and one of the key things is—I am a technologist. I love computers. I have a new iPad. People are the key to this, and good quality trained people is what our Nation needs in the National Security Agency and U.S. Cyber Command.

Senator HAGAN. Thank you, and I think that is critical. I think that national security is certainly interdependent on our education system, too. And I think the STEM program, science, technology, engineering, math, is something as a country we have got to be focused on.

So thank you very much.

Senator UDALL. Thank you, Senator Hagan.

I'm tempted to get a critical review of the iPad, but perhaps we can—

General ALEXANDER. Wonderful.

Senator UDALL. Wonderful. We'll put that for the record.

General, I'd like to talk more specifically about an area in our infrastructure world that could be vulnerable. There's been a lot of excitement about smart grids. I know Senator Hagan's been a leader in this area, and we see some real potential to lessen our dependence on foreign oil, use our energy that we have more effectively. But at the same time, I understand there are some vulnerabilities that may arise because of the deployment of the smart grid technologies. Would you care to comment?

General ALEXANDER. Senator, I'm a proponent for the smart grid and using some of this, but we have to walk into this with our eyes wide open. I think these information assurance programs between industry and government and understanding the full spectrum of threats that we face from individual hackers up to nation states in securing that are going to be key.

We all have a responsibility on the National Security Agency side and on the future Cyber Command side to help identify flaws in those, share those with industry and the Department of Homeland Security. But this is going to be an area, Senator, I think we're going to have to work in because it will always evolve. Someone will figure out a new way in and we've got to be there to close that gap.

Senator UDALL. I was listening to you earlier talk about defensive capabilities that exist today and the challenge we face with providing defensive tools and techniques. It seems to me—and I'm thinking out loud, which can be dangerous—that if you have a kinetic environment, say at a forward operating base in Afghanistan, if that base were to be overrun by the enemy in a tactical effort, it would not threaten the entire effort we have under way in Afghanistan. On the other hand, if you have a portal or an entry point that is the site of a tactical incursion in cyber space and that point is overrun in a tactical sense, it could have strategic ramifications that are much greater than those we might face on the ground in a place like Afghanistan.

Is that a fair characterization? Straighten me out, elaborate on that?

General ALEXANDER. Senator, that's absolutely right. General McChrystal has reached out to work with the other combatant commands, with us, with the National Security Agency, in building an Afghan mission network and ensuring that that network is secure, because it will not only be for the U.S. but the other coalition partners there.

There are a lot of issues in developing that that we're working through as a joint team. I think that's the first—you've hit it right on the head, because those communications bring in our intelligence, our operations, our logistics, and his ability to command and control all those forces across more than 40 countries. He has to ensure that those communications are reliable and protected. A huge issue and one of the key ones that we're working right now.

Senator UDALL. And this could be specific to Afghanistan, but if you penetrate, again, a network and a system anywhere in the world, it could then have effects anywhere else in the world. You alluded to this earlier, I think, when you talked about what defines a country, what is ground that we have to defend. That server that's being attacked could be in any number of countries or the attacker could be based in any number of countries. This raises some very thorny questions, does it not?

General ALEXANDER. Senator, it does. Those are the issues, the policies, that we have to I think address. It brings up issues such as attribution. It brings up the neutrality. I think our response we put in there, we are trained for proportional and discriminate, but there are still a number of issues that are out there. As you look at the complexity from mobile devices—we mentioned the iPad—

the tremendous capability you will have from mobile devices only makes this a more complex issue.

Senator UDALL. One of the arguments that has been brought forth about networks is that you get particular nodes cut off and the network itself can continue to operate. That concept's also being applied to kinetic activities on the ground in the kind of warfare we're now fighting. Would you elaborate a little bit more on that, that point as well?

General ALEXANDER. Senator, I think one of the difficult parts that we'll have is what are the actions of the adversary on our network? Is it exploitation or attack? Who is it, and attributing it and their intent, in time to come up with a coherent response. The easiest and the most important probably is the security aspects of it.

So if a system is exploited or has an infection, closing that off is one of the key things that we do early on, segregating that so it can't affect other—infect other systems. And the network can operate with several nodes out. That's the intent of a network for the future. But it also causes concern of what is the adversary's intent, what's his game plan, does he have one. So these are tough issues, especially when attribution and neutrality are brought in, and trying to figure out what's come in, was it a hacker, was it an annoyance, or was this a real attack?

Senator UDALL. The potential to generate an escalating conflict is not insignificant, much like we saw during the Cold War era with nuclear weapons. So I take your cautions with real seriousness.

Admiral, I haven't allowed you an opportunity to speak. Did you have any comments? I'm going to bring this hearing to a close here shortly, but I wanted to see if you had any additional thoughts.

Admiral WINNEFELD. Yes, sir. I was just reflecting on the fact that some of the questions you asked were very insightful in the sense of deterrence against a hard-to- deter nation in the cyber world, an empowered individual in the cyber world the same. We see the same thing with the sorts of terrorist attacks with potential nuclear, chemical, biological, or radiation.

I would also echo your point on the education piece. Educating citizens about the cyber world, the same thing applies in the kinetic world as well. So this phenomenon of a super-empowered individual is something that we have to be very watchful of.

Senator UDALL. It's a great concern to all of us. That super-empowered individual could have a goal of trying to trigger a significant conflict between nation states or other entities while he or she stands to the side chortling, with their mission to create chaos and conflict and tragedy and all the rest that we've seen in the toolbox that terrorists bring. So this is very important work you are doing.

One final question. General, I think you're going to be charged with further integrating and understanding these Title 10 and Title 50 responsibilities, are you not? We haven't answered all of those questions yet. You've certainly been at the forefront at NSA in taking on some of those challenges. You've at times received some criticism, I think we all have, because these are somewhat different missions, but they're certainly interlinked.

Would you care to comment?

General ALEXANDER. Senator, one of the key things that we're doing is we will have a unique set of authorities, a unique staff for Cyber Command operating under Title 10, and the National Security Agency, Central Security Service under Title 50. We do have some Title 10 responsibilities. We are a combat support agency. We do forward deploy people to help the combat, the regional combatant commanders. But there will be two distinct staffs, with distinct authorities and responsibilities for how we operate for intelligence, for information assurance on the NSA side, and for Cyber Command how we defend and secure our networks and conduct cyber space operations if directed.

Senator UDALL. I thank you for your focus on that. As somebody who's a strong supporter of our civil liberties, who believes that Ben Franklin had it right, to paraphrase him, when he said: A society that would sacrifice essential liberties for short-term security deserves neither. I think you're on the forefront, and Admiral Winnefeld as well, of protecting those civil liberties, but also surveiling and developing intelligence that lets us protect those very freedoms that we hold so dear.

So thank you both for being here. I'm going to bring the hearing to a close. Admiral, I think we ought to send one of your boys over to the U.S. House to demonstrate how to behave properly, and we'll keep one here in the United States Senate. It's been wonderful to have your family here, and General Alexander as well.

We will keep the record open for additional questions for a period of time. But with that, this hearing is adjourned. Thank you very much for being here.

[Whereupon, at 11:17 a.m., the committee adjourned.]