NOMINATIONS BEFORE THE SENATE
ARMED SERVICES COMMITTEE, SECOND SESSION, 111TH CONGRESS

HEARINGS BEFORE THE
COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE
ONE HUNDRED ELEVENTH CONGRESS
SECOND SESSION
ON
NOMINATIONS OF
ELIZABETH A. McGrath; Michael J. McCord; Sharon E. Burke; Solomon B. Watson; Katherine G. Hammack; VADM James A. Winnefeld, Jr., USN; LTG Keith B. Alexander, USA; Gen Raymond T. Odierno, USA; LTG Lloyd J. Austin III, USA; Gen David H. Petraeus, USA; Gen James N. Mattis, USMC; Jonathan Woodson, M.D.; Neile L. Miller; Anne M. Harrington; Gen. James F. Amos, USMC; Gen. Claude R. Kehler, USAF; and Gen Carter F. Ham, USA

March 23; April 15; June 24, 29; July 27; August 3; September 21; November 18, 2010

Printed for the use of the Committee on Armed Services

Available via the World Wide Web: http://www.fdsys.gov/
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, professional staff member; 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 J. Peterson, assistant to Senator Webb; Jennifer Barrett, assistant to Senator Udall; Nathan Davern, assistant to Senator Burr; 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.
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 and to be Commander of U.S. Northern Command (NORTHCOM) and Commander of the North American Aerospace Defense 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 (NSA), the Director of the Central Security Service, and to be Commander of the new U.S. Cyber Command (CYBERCOM).

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, North Atlantic Treaty Organization 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.

NORTHCOM, 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 latter mission requires a high level of cooperation and coordination with other Federal agencies and State agencies, especially the Department of Homeland Security (DHS).

The Commander of NORTHCOM 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 NORTHCOM area of responsibility (AOR). 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, NORTHCOM 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 U.S. Central Command; Commanding General for
the Army Intelligence and Security Command; and the Deputy Chief of Staff of the Army for Intelligence before becoming Director of NSA in 2005.

With respect to the position to which General Alexander has been nominated, the creation of a new combatant command, even at the subunified level, is an extremely important matter. The creation of CYBERCOM 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 development 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 U.S. 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 subunified combatant commander.

Faced with that complex situation, the committee proceeded methodically to gain an understanding of what 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 (DOD) 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 DOD's leadership and the administration as a whole is committed to rapidly closing the cyber space policy gap. The committee has also been assured that DOD 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 M. 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, CYBERCOM 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 CYBERCOM 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 to ensure that DOD, 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 websites 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 2007 to appreciate the nature of this form of modern warfare.

We look forward to your testimony about how CYBERCOM 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 NORTHCOM and NORAD. The vicious attacks of September 11 are never far from our thoughts. Ensuring 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 NORTHCOM 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 policy 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. The drug-related violence in Mexico is appalling. As you
noted, there were over 6,500 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; of Jorge Salcido, the husband of a U.S. consulate employee; and the murder of Robert Krentz, a rancher in Douglas, AZ, 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 Jan 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.

Mr. Chairman, I’d like to insert two letters into the record: one I wrote to Secretary Napolitano on March 29; and the other addressed to the mayor of Douglas, AZ, on March 31 in this regard.

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

[The information referred to follows:]
United States Senate

March 29, 2010

The Honorable Janet Napolitano
Secretary
U.S. Department of Homeland Security
Nebraska Avenue Complex
245 Murray Lane, Mailstop 0150
Washington, DC 20528-0150

Dear Secretary Napolitano,

I am gravely concerned with the continued and apparently growing violence along our border with Mexico. Most recently, I was saddened and outraged to hear of the death of Robert Krenz, a longtime Arizona rancher who was found dead on his property near Douglas, Arizona. The federal government must do all it can within its power to curb this violence and protect its citizens from criminals coming across the border from Mexico.

For years, I have called on the President to send National Guard troops to the border in an effort to stop the flow of illegal immigrants and narcotics. Most recently, I supported Governor Jan Brewer's request to place troops along Arizona's border with Mexico. Unfortunately that request was rejected by this Administration. A year later, in light of the recent incidents and the continued growth of drug violence along the border, I am asking you and the Administration to immediately reconsider your position and send National Guard troops to our southern border region.

We must make the security of our borders one of our top national security priority. The United States must also do all it can to assist the Mexican government in its efforts to combat these violent drug cartels. The prosperity and success of Mexico is essential to the prosperity and success of our own country. We share a border, our economies are intertwined, and we are major trading partners. The U.S. must show its support for our neighbor to the south and support the Mexican people and the Calderon Administration in this fundamental struggle against lawlessness and corruption.

The people of Arizona and the United States demand and deserve secure borders. I hope that you will take a personal interest in ensuring that Arizonans can feel safe and protected on their own property and not live in fear of the increasing violence along the border. I look forward to a swift and decisive response to this situation.

Sincerely,

John McCain
U.S. Senator
United States Senate

March 31, 2010

Dr. Michael Gomez
Mayor
425 East 10th Street
Douglas, Arizona 85607

Dear Dr. Gomez:

Thank you for your letter dated March 30, 2010 regarding the tragic death of Rob Krentz, a respected member of our community and proud Arizonan. Please accept my sincere condolences on the loss of this esteemed community leader, husband and father.

As you know, over the years, I have continually raised concerns about the security of our southern border. Securing our border has been, and remains, a national priority that must be immediately and urgently addressed. Unfortunately, to date, not enough has been done. Rhetoric must be put aside and we must act decisively before any more residents of our border states are subjected to the tragedy that befell the Krentz family.

I wanted to take this opportunity to respond to your letter and let you know what efforts are being taken at this time to address at least some of your concerns. I have been in touch with numerous Federal, state and local law enforcement officials since this horrific crime and want to share with you what I have learned. The Department of Homeland Security (DHS) has pledged to immediately send more border patrol agents to secure the border between Cochise County, Arizona and Mexico. I believe this “border patrol agent surge” will immediately improve the safety and security of all residents of Douglas and the surrounding communities.

Additionally, the Commissioner of the Customs and Border Patrol, Alan Bersin, has been in direct contact with Cochise County Sheriff Larry Dever and pledged any resources necessary to assist Sheriff Dever in his work. This afternoon, Immigration and Customs Enforcement announced a $25,000 reward for the capture of the suspect alleged to have shot Mr. Krentz. Also, as you may be aware, on Monday, I wrote Secretary Napolitano and strongly reiterated my request originally made last year that the Federal government immediately send the National Guard to the border to support the DHS’s efforts.
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.

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 unmanned aerial vehicles (UAVs), and better ways to enforce our border and make sure that it is secure. 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.

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.

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? 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, Mr. Chairman, Ranking Member McCain, and colleagues. I have the opportunity today to introduce Lieutenant General Keith Alexander, who is the current Director of NSA, located in Fort Meade, MD. I also am very proud to sit here today with Admiral Winnefeld, and I would like to re-echo 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 mothership of signals intelligence in the U.S. military, which is NSA. I would recommend in a classified hearing that the scope, breadth, and talented workforce, 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 CYBERCOM. 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 CYBERCOM, 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 dot-com 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, 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 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 NSA 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 sup-
porting the wars in Iraq and Afghanistan, working with NORTHCOM and our forces at the border protecting our borders.

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 workforce 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 CYBERCOM 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. He’s been a promoter of innovation.

I come to this because the committee 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 CYBERCOM and we need the leader who has 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:]

PREPARED STATEMENT BY SENATOR BARBARA MIKULSKI

Thank you Chairman Levin and Ranking Member McCain for the opportunity to introduce Lt. Gen. Keith Alexander, the current Director of the National Security Agency (NSA), located in Fort Meade, MD.

As the Senator from and for Maryland, I am pleased and honored to introduce Lieutenant General Alexander to the Senate Armed Services Committee for his confirmation hearing to lead Cyber Command. In October 2009, President Obama, with the support and backing of Defense Secretary Gates and Director of National Intelligence (DNI) Blair, nominated Lieutenant General Alexander to lead Cyber Command.

I have known Lieutenant General Alexander since he started as Director of the NSA in 2005. Lieutenant General Alexander’s leadership and expertise as Director of the NSA for the past 5 years, Deputy Chief of Staff of the Army, General of the U.S. Army and Intelligence and Security Command, Director of Intelligence, U.S. Central Command and numerous other positions make him uniquely qualified to lead Cyber Command.

Lieutenant General Alexander has led the transformation of the NSA from an agency focused on counter-terrorism into an organization that is leading the fight against cyber spies who want to steal our State secrets, cyber terrorists who want to disrupt our power grid and cyber criminals who want to make a quick buck, all while still supporting the wars in Iraq and Afghanistan. Lieutenant General Alexander is a leader, a professional and, most important for this job, he is an indispensable asset to our Nation’s cyber security.

As a member of both the Intelligence Committee and Defense Subcommittee on Appropriations, which funds the NSA, I have seen the tremendous things that the NSA is doing in cyber space both to protect our national security systems and to keep us ahead of our cyber adversaries.

The United States is being hacked and being attacked by cyber adversaries and foes each and every day. Cyber spies want to steal our State secrets, weapons systems, and restricted technology. Cyber hackers who want to make off with our intel-
lectual property and patents and cyber criminals who want to make a quick $10,000.

Our cyber shield is thinning and a unified response is necessary. The U.S. military needs a unified effort—a Cyber Command—to have the ability to respond with speed, agility, and flexibility to increasingly sophisticated cyber adversaries.

As DNI Mike McConnell—a former NSA Director himself—once told me, Lieutenant General Alexander is an asset to our national security, and I agree with him. Cyber hackers and warriors continue to hack and attack us each day. Cyber hackers and warriors are operating with increasing speed and sophistication.

This nomination is one that cannot wait. I strongly support his nomination to lead Cyber Command and I urge his quick confirmation.

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 intended to set out at least, some of the very significant issues that this new command raises. But your eloquence is very helpful in this regard and your comments are very welcome.

Senator Mikulski. Good luck. I have 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, NOMINEE TO BE ADMIRAL AND COMMANDER, U.S. 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 NORTHCOM and the Commander of NORAD. 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, WI, 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 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 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.

If confirmed, I will reinforce the critical importance of close partnerships and teamwork with the other combatant commanders and Service Chiefs, with DHS, and a host of other interagency, 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 important 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.

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, NOMINEE 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, NSA; Chief, Central Security Service; and for Commander, CYBERCOM. 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 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, terrorists, criminal groups, and individual hackers,
who are capable of stealing, manipulating, or destroying information that could compromise our personal and national security. DOD 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 CYBERCOM 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 (STRATCOM) 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 CYBERCOM 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 CYBERCOM, 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 CYBERCOM and NSA 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.

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 4 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,
and cyber doctrine. You as the first Commander of CYBERCOM 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; 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's what I wanted to do because I wanted you to be able to know in advance 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.

Let me give you the hypotheticals, starting with the easiest one, I think, which is assume the following: 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 authorities, processes, and orders would you be operating in that particular scenario? 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.

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 STRATCOM, 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, 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. There would be a rules of engagement that articulate what you can do offensively and what you can do defensively. Sir, in offense that's both in the exploitation and in the attack role. 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. Neutral being a third country, presumably? Is that synonymous or does the word "neutral" mean literally neutral?

General Alexander. 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. 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. That's the complexity that you've addressed.

Now a third scenario, more complicated yet. Assume you're in a peacetime setting. 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. 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.

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, DHS would have the responsibility for the defense of that working with critical infrastructure. DHS could, through the defense support to civilian authorities, reach out to DOD and ask for support. Sir, one of our requirements in the unified command plan is to be prepared for that task. 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 interagency 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 interagencies working together with industry. I think that’s one of the things that the administration is trying to address with DHS and with DOD, 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 DOD help DHS 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 it what the hope is, the goal is, for that?

General Alexander. I think DOD 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 GMD 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 GMD system that I referred to.

But first, do you agree 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 United States 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 intercontinental ballistic missile capability is an adjunct to that.

Chairman Levin. 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 Senate Homeland Security and Governmental Affairs 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 Congress, for us to 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 and effective fashion?

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

[The information referred to follows:]

[Deleted.]

Senator McCain. I think it's obvious from General Alexander's testimony that close coordination between DHS and DOD is critical in taking effective measures in this new cyber war that we are in.

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 and Governmental Affairs 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, whom 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 the early stages of my assessment, to be quite honest with you. In preparation for the hearing, I have 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.

Senator MCCAIN. 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 scrutinize more carefully and utilize some of the lessons we have learned in, say, Iraq. 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 UAVs, surveillance capabilities, as well as barriers. We all know that barriers only work if they are surveilled 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 an obligation to secure our borders to prevent further incidents such as the murder of a rancher in Douglas, AZ, just a short time ago.

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 down near the border and some of the illegal activity has affected our training capabilities there. There are 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, 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 request has not been met with a favorable response as of yet.

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. If they're not losing in any war, then they are winning. This is an irregular warfare 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.

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

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. 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 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 comply 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. Yes, sir.
Chairman Levin. Do you agree, if confirmed, to appear and testify upon request before this committee?
General Alexander. Yes, sir.
Admiral Winnefeld. Yes, sir.
Chairman Levin. Finally, do you agree to provide documents, including copies of electronic forms of communications, in a timely manner when requested by a duly constituted committee or to consult with the committee regarding the basis for any good faith delay or denial in providing such documents?
Admiral Winnefeld. Yes, sir.
General Alexander. Yes, sir.
Chairman Levin. Thank you very much.
Senator Lieberman.
Senator Lieberman. Thank you, 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, as we stand up this new CYBERCOM and you as its first leader, how serious is the cyber threat to the United States today? To the extent that you're able to say in open testimony, particularly about DOD 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 DOD 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? By putting the command together, I think that was what he saw as the first big step that we need to make to build the capacity and to take that on. 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 DOD. So it's growing rapidly.

Senator LIEBERMAN. Right. 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. 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 DOD and DHS because, as Senator McCain said, I'm privileged to be chair of the Senate Homeland Security and Governmental Affairs Committee. There's a lot of overlap, not surprisingly, between the membership on these two committees.

The existing system allocates responsibility between DOD and DHS, DOD obviously having responsibility not only for offensive cyber operations, but for the defense of DOD's networks. DHS 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 DHS in enabling its work. The bottom line here is that the NSA is a treasure, a national treasure. Its resources are extensive. No one I think would want DHS to try to replicate those resources to carry out its responsibility to protect Federal Government civilian networks and outside civilian networks.

Therefore the cooperation is really critically important. Can you explain both what that relationship is now and how you envision CYBERCOM that you'll now head and NSA playing a supporting role to DHS in protecting non-military networks?

General ALEXANDER. Senator, I'm going to break that into two parts, one that talks about what NSA is doing to support DHS 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 DHS. We do that under 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 part of the issue, as you can see. 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 CYBERCOM side, if a crisis were to occur, now CYBERCOM or DOD 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 NORTHCOM, it could go to STRATCOM or to CYBERCOM to provide either technical support or help prevent an attack, or in the case of a sustained attack actually help defend our networks.

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 CYBERCOM would come in and work with DHS 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, CYBERCOM, NSA, and DHS is a good one? Understanding that you have 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 DOD components to better assist DHS in its cyber security mission.

General ALEXANDER. Yes, sir.
Senator LIEBERMAN. Thank you.
Thank you, 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 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 of-

cine, I'm on the 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. 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 Information
Technology (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 con-
cerned about that.

I've been told that 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.

Second, I want to talk about some of the systems outside of the
military that I'll be asking you about, due to something that ap-
peared this morning in the media. Does 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 prob-
lems do you see that you haven't already mentioned in the previous
questions?

Again, I apologize for not being here for your opening statement,
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 offensive and defen-
sive 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. This was separated in responsibilities be-

tween 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, and 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 guard for those exploits or attacks into our network.

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

This morning on Dark Reading—it's a business IT web site—they talk about, even with minimal Internet access, malware and breaches are increasingly occurring. We're talking about the non-military, nondefense 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 do you anticipate to do—you've talked about the problems that are out there—in terms of approaching those problems, finding solutions? 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 nonmilitary, nondefense 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 DHS, who has the lead in this area with civilian industry, with DOD and the Intelligence 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. You're the right person for it. I'm glad that you're doing what you're doing. 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 concerned when that was pulled out from under them a year ago in the first budget of this administration.
Now, 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, 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, is that it 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, where that could be deployed?

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

Senator INHOFE. I know that.

Admiral WINNEFELD. 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? 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. 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. 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. My time has expired, but when you say the percentages will go up, that’s something you can’t talk about in an open meeting. 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. I'm sure we'll have a chance in the days ahead to talk seriously about these very critical issues. Thank you for your service.

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 NORTHCOM. Can you tell 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. When you look at the fact that NORAD might be providing some aerospace warning of, for instance, the ballistic missile threat, that then NORTHCOM 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, CYBERCOM and NSA. You talked about your understanding of the importance that oversight transparency will play in this new structure. Yet in the advance policy questions you were only able to provide classified answers to what seemed to be some of the fundamental challenges facing CYBERCOM. 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 NSA side to support that and what we do on the CYBERCOM side. The reason I say that, I believe that the Government combined, Congress and the administration, to the American people, we have 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 CYBERCOM as well to ensure that we have those same things.

It seems to me 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 CYBERCOM and NORTHCOM. 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 DHS 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 DHS do their mission.

Senator Udall. Admiral, would you care to comment?

Admiral Winnefeld. 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 interagency 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 DHS in the lead. But he will be an integral player in that process. 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. 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."

That statement leaves me 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 United States 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. The issue is from a military perspective, if these things are impacting our networks today we have a responsibility to defend those and set up cyber security.

I think the steps that we’re taking with CYBERCOM 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 CYBERCOM 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 Chief Executive Officer (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 part of the issue, 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 DHS has a tough set of issues. In crisis, that’s where calling between DHS and DOD, 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 trying 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 have 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 DHS, a team, how we’re doing it and ensure 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. 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 better job. Thank you to all of the families.

I also wanted to say I thought Senator Mikulski’s introduction was right on. We always enjoy hearing Senator Mikulski.

Admiral Winnefeld, many defense analysts have noted that it’s time for the Nation to look beyond 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 NORTHCOM, 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 DOD and DHS 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 DHS 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, exercise and training, and operational execution levels.

At the planning levels, a lot of collaboration is going on, prescribed mission assignments that DHS 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 well. There are liaison officers from DHS 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. 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. 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 servicemembers 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.

Admiral Winnefeld, in the event that an equally devastating earthquake or hurricane were to strike here in the United States, 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 have 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 Airland 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 Arkansas without consulting the affected adjutant generals or State Governors. Obviously, North Carolina is one of the States where this is being discussed.

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 adjutant generals,
to ensure that we have a very clear understanding and that they know that I'm a believer in 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 CYBERCOM. 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 NSA, Chief of Central Security Service, and Commander of CYBERCOM, 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 NSA. They have great people, tremendous people. Our Nation has put a lot into building NSA 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 CYBERCOM 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.

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 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 workforce that you're seeing and where you're recruiting individuals? If there is 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 science, technology, engineering, mathematics (STEM). I think it's abo-
lutely 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 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 CYBERCOM 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 DHS 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 have 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 NSA and CYBERCOM.

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

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, 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 NSA side and on the future CYBERCOM side to help identify flaws in those, share those with industry and DHS. 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 have 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 ki-
netic 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 NSA, in building an Afghan mission network and ensuring that network is secure, because it will not only be for the United States but the other coalition partners there.

There are a lot of issues in developing that we’re working through as a joint team. I think 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. 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.

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 infect other systems. 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. 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. 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. 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, conflict, 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 CYBERCOM operating under title 10, and the NSA, 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 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 CYBERCOM 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 surveilling and developing intelligence that lets us protect those very freedoms that we hold so dear.

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 of Representatives to demonstrate how to behave properly, and we'll keep one here in the U.S. 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.]

[Prepared questions submitted to VADM James A. Winnefeld, Jr., USN, by Chairman Levin prior to the hearing with answers supplied follow:]

**QUESTIONS AND RESPONSES**

**DEFENSE REFORMS**

**Question.** The Goldwater-Nichols Department of Defense Reorganization Act of 1986 and the Special Operations reforms have strengthened the warfighting readiness of our Armed Forces. They have enhanced civilian control and the chain of command by clearly delineating the combatant commanders’ responsibilities and authorities and the role of the Chairman of the Joint Chiefs of Staff. These reforms have also vastly improved cooperation between the Services and the combatant commanders, among other things, in joint training and education and in the execution of military operations.

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

**Answer.** I have served in various joint capacities throughout my naval career and witnessed firsthand the tremendous advancements this landmark legislation has created, not only among our Nation’s military and civilian leadership, but as a whole within the joint services and interagency environment. As such, I do not see an immediate need to change the provisions of this legislation. However, if confirmed, I will take a hard look at ways Northern Command (NORTHCOM) does business to determine if changes in the legislation are warranted.

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

**Answer.** Not applicable.

**DUTIES**

**Question.** What is your understanding of the duties and functions of the Commander, NORTHCOM?

**Answer.** The Commander of NORTHCOM is responsible for detecting, deterring and preventing threats to the people and territory of the United States; providing military support to Federal, State and local authorities in response to natural or manmade disasters or for other missions, as directed by the President or the Secretary of Defense; and executing theater security cooperation programs with Mexico, Canada and the Bahamas.

**Question.** What is your understanding of the duties and functions of the Commander, North American Aerospace Defense Command (NORAD)?

**Answer.** The Commander of NORAD is responsible to both the President of the United States and the Canadian Prime Minister for aerospace warning, aerospace control and maritime warning of North America. The Commander of NORAD provides tactical warning and attack assessment to the Governments of the United States and Canada through an integrated picture of any aerospace threat.

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

**Answer.** It has been my honor to serve for over 30 years in a diverse set of positions that I believe have prepared me to command NORTHCOM and NORAD. Given my background as a naval aviator, I will bring both an air and maritime perspective to the two commands. I have experience on Joint Staff, Combatant Command, and Service staffs, served as both a joint and combined commander, and have worked closely with Congress on a variety of issues. In my current position as the Director for Strategic Plans and Policy on the Joint Staff, I have gained additional insight into the conduct of joint, combined and international operations; the duties of a combatant commander; the importance of interagency teamwork, particularly in response to natural disasters; and the critical role of the National Guard and Federal Reserve forces in defending our homeland and supporting civil authorities in times of crisis.
**Question.** Do you believe that there are any steps that you need to take to enhance your expertise to perform the duties of the Commander, NORTHCOM and Commander, NORAD?

**Answer.** If confirmed, I intend to capitalize on every opportunity to further my understanding of NORTHCOM's homeland defense and civil support operations; specifically, how the National Guard and Federal Reserve forces contribute to those missions and the whole-of-government approach to responding to natural and man-made disasters. This includes maintaining strong relationships with the Adjutants General, State Governors, and the leadership of key Federal agencies.

I also intend to deepen my growing knowledge of the threat posed to the United States and our neighbors by drug trafficking organizations, as well as existing strategies to defeat them.

If confirmed in my role as Commander of NORAD, I will continue to expand my knowledge of NORAD's aerospace warning, aerospace control, and maritime warning operations and how the command integrates with its partners to detect, intercept and, if necessary, engage any air-breathing threat to North America. Additionally, I will receive the same training provided to other NORAD senior leaders required to direct the actual, formal process of engaging aerospace threats to our Nation.

**RELATIONSHIPS**

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

**Question.** The Secretary of Defense.

**Answer.** The Commander of NORTHCOM has direct Title 10 responsibility to the Secretary of Defense for accomplishing the missions assigned to the command through the Unified Command Plan. If confirmed, I will ensure NORTHCOM continues the close working relationship it currently has with the Secretary of Defense.

**Question.** The Deputy Secretary of Defense.

**Answer.** The Commander of NORTHCOM provides the Deputy Secretary of Defense information required to accomplish his duties and responsibilities as directed by the Secretary of Defense. The Commander of NORTHCOM also coordinates with the Under Secretary of Defense for Policy on major homeland defense and civil support issues.

**Question.** The Under Secretary of Defense for Policy.

**Answer.** The Under Secretary of Defense for Policy serves as the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for all matters on the formulation of national security and defense policy and the integration and oversight of DOD policy and plans to achieve national security objectives. She is also a key advocate for NORTHCOM's requirements. As such, the Commander of NORTHCOM coordinates and exchanges homeland defense, support of civil authorities, and security cooperation information with the Under Secretary of Defense for Policy in formulating planning guidance and policy.

**Question.** The Under Secretary of Defense for Intelligence (USD(I)).

**Answer.** The USD(I) is the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense regarding intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters. The Commander of NORTHCOM works closely with the Under Secretary of Defense for Intelligence to ensure the command has predictive and actionable threat estimates and timely warning of worldwide threats to the homeland.

**Question.** The Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs.

**Answer.** The Commander of NORTHCOM routinely works with the Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs on significant matters regarding homeland defense, support of civil authorities, and security cooperation.

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

**Answer.** The Chairman serves as the principal military advisor to the President, the Secretary of Defense, and the National Security Council. The Goldwater-Nichols DOD Reorganization Act of 1986 permits the President to place the Chairman in the communications chain, and oversight of the activities of combatant commanders may be delegated by the Secretary of Defense to the CJCS. In concert with this authority, the Commander of NORTHCOM communicates closely with the Chairman.
to enable him to perform his duties. As the current Director for Strategic Plans and Policy for the Joint Staff, I have been deeply involved in interactions between the Chairman and combatant commanders, and understand the process well.

**Question.** The Secretaries of the Military Departments.

**Answer.** The Secretaries of the Military Departments are responsible for organizing, training, and equipping forces for assignment to the Commander of NORTHCOM and other combatant commanders. The Commander of NORTHCOM coordinates with the Secretaries to ensure homeland defense and civil support requirements are met. This advocacy is particularly important for ensuring the Reserve component is ready to answer the call here at home, and for ensuring speed of response in times of crisis.

**Question.** The Chiefs of Staff of the Services.

**Answer.** The Commander of NORTHCOM communicates with the Chiefs of Staff of the Services to support their responsibility for organizing, training and equipping forces to accomplish homeland defense and civil support missions. In addition, the NORTHCOM Commander seeks the advice and judgment of the Chiefs of Staff on matters of mutual interest, and has a key relationship with the Chiefs on matters of force protection within his area of responsibility. If confirmed, I intend to rely on the Service Chiefs as valuable sources of advice.

**Question.** The other combatant commanders, particularly U.S. Southern Command (SOUTHCOM).

**Answer.** The Commander of NORTHCOM communicates with the Chiefs of Staff of the Services to support their responsibility for organizing, training and equipping forces to accomplish homeland defense and civil support missions. In addition, the NORTHCOM Commander seeks the advice and judgment of the Chiefs of Staff on matters of mutual interest, and! has a key relationship with the Chiefs on matters of force protection within his area of responsibility. If confirmed, I intend to rely on the Service Chiefs as valuable sources of advice.

**Question.** The Chief of the National Guard Bureau.

**Answer.** Strong teamwork between the National Guard Bureau and NORTHCOM is critical to defending our homeland and supporting civil authorities. In my current position as Director for Strategic Plans and Policy for the Joint Staff, I have developed a strong belief in the vitality of the National Guard, and enjoy an excellent relationship with the Chief of the National Guard Bureau, General Craig McKinley. If confirmed, I look forward to further advancing this key relationship so together we may best serve the American people.

**Question.** If confirmed, in carrying out your duties, how would you work with the Department of Homeland Security, the Homeland Security Council, and other Federal agencies, as well as State and local authorities and representatives from the private sector?

**Answer.** From my vantage point on the Joint Staff, I have observed NORTHCOM successfully operate within the most complex interagency network of any combatant command. If confirmed, I will establish my own relationships with—and ensure NORTHCOM continues to work issues closely and as appropriate with—the National Security Council; the Department of Homeland Security; the various other Federal departments and agencies; State, tribal and local authorities; and the private sector. I look forward to collaborating with every possible partner to defend the homeland while ensuring that NORTHCOM is fully prepared to assist civil authorities in support of the primary Federal agency in accordance with the National Response Framework and as directed by the President and the Secretary of Defense.

**MAJOR CHALLENGES AND PROBLEMS**

**Question.** In your view, what are the major challenges that will confront the next Commander, NORTHCOM?

**Answer.** I believe one of our Nation's most serious security challenges is protecting the United States from an attack by violent extremists using weapons of mass destruction; accordingly, this is one of NORTHCOM's enduring challenges. I am increasingly concerned by the evolving nature of this extremist threat towards smaller scale, hard-to-detect operations. This threat is determined and patient, will attempt to use our freedoms against us, will search for any path to produce violent events, and harbors no qualms about killing innocent men, women, and children to achieve its objectives.

I am also concerned about the corrosive effect on our nation's security of drug trafficking, including its associated violence both inside Mexico and along our border.
If confirmed, I will ensure NORTHCOM continues to support a whole-of-government approach on both sides of our border with Mexico and in strengthening Mexico’s ability to reduce and minimize this violence by dismantling and defeating transnational drug trafficking organizations.

In the longer run, I am concerned about the potential acquisition by rogue nations, such as North Korea and Iran, of the combination of a nuclear weapons capability and the capacity to deliver it to our shores. Finally, the constant potential for a major natural disaster is something for which the NORTHCOM Commander must always be prepared.

**Question.** Assuming you are confirmed, what plans do you have for addressing these challenges?

**Answer.** If confirmed, I will do everything in my power to ensure our Nation is prepared to handle the full spectrum of threats to our homeland. I will be an advocate for the sense of urgency required to maintain vigilance against these threats; nurture a culture that continuously challenges and improves our capability, particularly in the area of information sharing with our partners; and continue improvements to NORTHCOM’s rigorous exercise program. I will examine the command’s homeland defense and civil support plans to ensure they address evolving threats and are tailored to need. I will continue to strengthen NORTHCOM’s relationships with its National Guard, interagency, State, local, tribal, and international partners to ensure the whole is greater than the sum of the parts.

**MISSION OF NORTHERN COMMAND**

**Question.** What is the mission of NORTHCOM?

**Answer.** NORTHCOM anticipates and conducts homeland defense and civil support operations within its assigned area of responsibility in order to defend and secure the United States and its interests. In addition, the command is responsible for executing theater security cooperation with Mexico, Canada, and the Bahamas, with full respect for their sovereignty.

**Question.** How does NORTHCOM’s mission relate to the mission of the Department of Homeland Security?

**Answer.** The Department of Homeland Security is responsible for guarding against terrorism; securing our borders; enforcing our immigration laws; and improving our readiness for, response to, and recovery from natural and man-made disasters. NORTHCOM is responsible for detecting, deterring, and preventing external threats to the United States, and when directed by the President or Secretary of Defense, providing defense support of civil authorities (DSCA). NORTHCOM cooperates closely with—and for DSCA missions will be in support of—the Department of Homeland Security in the execution of its missions in accordance with direction from the President or the Secretary of Defense.

**Question.** Are there circumstances under which you would anticipate NORTHCOM would have the lead Federal role in responding to a terrorist incident?

**Answer.** Normally, the DOD (including NORTHCOM) will be in support of agencies such as the Department of Homeland Security, the Department of Justice, and the Federal Bureau of Investigation in preventing, countering, and responding to terrorist incidents in the United States. However, the President may determine that a terrorist incident rises to the level of an armed attack against the United States and therefore direct that DOD take the lead in the defense of the Homeland. The Commander of NORTHCOM, as the Geographic Combatant Commander, would likely be assigned as the supported DOD commander.

**Question.** Or do you believe NORTHCOM would operate only in support of other Federal departments and agencies?

**Answer.** See previous answer.

**Question.** What responsibility, if any, does NORTHCOM have with respect to the Defense Critical Infrastructure Program?

**Answer.** In accordance with the Secretary of Defense’s January 2010 directive on critical infrastructure, as a regional combatant command, NORTHCOM is responsible for preventing or mitigating the loss or degradation of DOD-owned critical assets within its area of responsibility.

**ORGANIZATION AND AUTHORITY**

**Question.** NORTHCOM has been assigned responsibility for force protection and antiterrorism within its area of responsibility. What actions would you take, if confirmed, to mitigate force protection vulnerabilities, and what force protection challenges do you anticipate you would face within NORTHCOM’s area of responsibility?
Answer. If confirmed, I will employ an all-hazards approach to force protection. I also understand that it is challenging to strike the right balance between threat mitigation, responsible stewardship of resources, and installation efficiency—areas that depend upon robust DOD and interagency coordination to provide for mission assurance at over 2,500 installations located in the NORTHCOM area of responsibility. If confirmed, I will make a concerted effort to determine where we stand on this key issue, and continue the command’s ongoing efforts to mitigate force protection vulnerabilities.

Question. What actions would you take, if confirmed, to ensure efficiency in the use of funding for force protection and to prevent unnecessary duplication of efforts between NORTHCOM, the Military Services, and the Office of the Assistant Secretary of Defense for Homeland Defense?

Answer. If confirmed, I will emphasize coordination among NORTHCOM, the Joint Staff, the Services, and the Assistant Secretary of Defense for Homeland Defense and America’s Security Affairs on force protection planning and resourcing to maximize efficiency and preclude redundant efforts. In addition, I will focus the command’s ongoing efforts to share force protection information to support critical analysis, as well as employing force protection and biometric technologies that are state-of-the-art and cost effective.

Question. What specific forces, if any, have been assigned to NORTHCOM?

Answer. The forces assigned to NORTHCOM are those inherent within the Headquarters staff, as well as the staffs of the subordinate/component commands listed below:

- U.S. Army North
- Marine Forces North
- Air Forces Northern
- Joint Task Force Civil Support
- Joint Task Force North
- Joint Force Headquarters National Capital Region

Question. How has the assignment of forces to NORTHCOM changed since NORTHCOM was established on October 1, 2002?

Answer. On 1 October 2003, when Full Operational Capability was achieved, the forces assigned to NORTHCOM consisted of the Service component headquarters and two standing Joint Task Force headquarters. In 2004, the command stood up a third Joint Task Force, Joint Force Headquarters National Capital Region.

On 1 October 2008, NORTHCOM was assigned forces in support of the standing Chemical, Biological, Radiological, Nuclear, and High Yield Explosive (CBRNE) Consequence Management Executive Order for a period of 12 months (October 2008 to September 2009). On 1 October 2009, the status of the CBRNE Consequence Management forces was changed back to allocated vice assigned, per the 2010 Global Force Management Allocation Plan.

NORAD

Question. What is the mission of the NORAD?

Answer. NORAD is charged with the missions of aerospace warning, aerospace control, and maritime warning for North America. Aerospace warning includes the detection, validation, and warning of attack against North America whether by aircraft, missiles, or space vehicles, through mutual support arrangements with other commands. Aerospace control includes ensuring air sovereignty and air defense of the airspace of the United States and Canada. Maritime warning consists of processing, assessing, and disseminating maritime intelligence and information, and warning of maritime threats to or attacks against, North America.

Question. How has NORAD’s mission evolved since the creation of NORTHCOM?

Answer. Since NORTHCOM stood up in 2002, NORAD’s mission expanded in two areas: maritime warning and ballistic missile warning. The April 2006 NORAD Agreement renewal added a maritime warning mission, which entails a shared awareness and understanding of the activities conducted in U.S. and Canadian maritime approaches, maritime areas and inland waterways. NORAD also provides ballistic missile warning to NORTHCOM in support of Ground-Based Midcourse Defense operations. Additionally, NORAD has been instrumental in rapidly developing a close operational relationship between NORTHCOM and Canada Command, the Canadian equivalent to NORTHCOM, which was established in 2005.

Question. How does NORAD’s mission relate to NORTHCOM’s mission?

Answer. NORTHCOM and NORAD are separate commands; neither is subordinate to the other. The commands have complementary missions, operate within a common security environment, and share a largely integrated headquarters staff. NORTHCOM is committed to the defense of the United States and NORAD is com-
mitted to the air defense of and maritime warning for both the United States and Canada.

**Question.** How does NORAD’s mission relate to the mission of the Department of Homeland Security?

**Answer.** NORAD, by performing its bi-national defense mission, provides significant but indirect support to the Department of Homeland Security by deterring threats in the air and maritime domains.

**Question.** Do you believe that NORAD should continue to have a combined operations and planning staff, and a consolidated command center, with NORTHCOM? Why or why not?

**Answer.** I understand that the NORAD and NORTHCOM staffs are fully integrated, with the exception of separate operations directorates, and that both commands believe this is effective. In my experience, where organizations are integrated well, greater effectiveness and efficiency can be the result. If confirmed, I will examine whether this organizational structure maximizes the operational effectiveness of both commands.

### NORTHCOM JOINT TASK FORCES

**Question.** Since the establishment of NORTHCOM, several multi-service task forces, e.g., Joint Task Force-Civil Support (JTF-CS), Joint Task Force-North (JTF-North), have been placed under its authority.

What is the current status of the Joint Task Force organizations under NORTHCOM in terms of organization, planning, personnel allocation, and capability?

**Answer.** NORTHCOM currently has three Joint Task Forces:

- Joint Task Force Civil Support: Aligned under U.S. Army North; provides command and control of DOD incident management forces that respond to catastrophic CBRNE events.
- Joint Task Force North: Aligned under U.S. Army North; supports counterdrug and border patrol support along the United States-Canada and southwestern U.S. border, and other operations against transnational threats.
- Joint Force Headquarters National Capital Region: Provides land-based homeland defense, civil support, and incident management in the National Capital Region.

Joint Task Forces under NORTHCOM’s authority are well-manned multi-service organizations that plan and execute Homeland Defense and Defense Support of Civil Authorities operations, as directed by the President or the Secretary of Defense. Joint Task Force operational planning is synchronized through continuous development and coordination of Joint Task Force plans that support NORTHCOM concept plans. These Task Forces further develop and refine plans, and exercise with HQ NORTHCOM, to enhance execution of existing and emergent homeland defense and civil support missions.

### COUNTER-NARCOTICS EFFORTS

**Question.** Each year the Department of Defense (DOD) spends several hundred million dollars to counter the flow of illegal drugs into the United States, yet the availability of drugs on the street has not been significantly reduced, and some countries continue to face internal security challenges in responding to this threat. Some of these funds are executed within the NORTHCOM AOR, and some have questioned the effectiveness and focus of our counter-narcotics programs.

What role does NORTHCOM play in the DOD’s overall counterdrug mission and organization?

**Answer.** DOD supports the counterdrug mission in both domestic and international environments, fully respecting jurisdictional and sovereignty restrictions in each area. NORTHCOM plays an integral role in these efforts, including cooperating closely with SOUTHCOM and PACOM in sharing information and situational awareness of drug-related threats to U.S. national security.

**Question.** NORCOM’s Joint Task Force North provides DOD support of civil authorities for U.S. law enforcement agencies in counternarcotics operations, as well as working with Mexican military and civil authorities along the border to enhance their capability. NORTHCOM is working with Mexico as it continues to build their overall capability and capacity to fight drug trafficking organizations as part of DOD’s support to the Mérida Initiative. NORTHCOM also partners with Canada and with the Bahamas on counterdrug matters.
Question. What is your assessment of the ongoing counternarcotics operations within the NORTHCOM AOR and the geographic seam NORTHCOM shares with U.S. Southern Command (SOUTHCOM)?

Answer. Interdicting drug flow in the Western Hemisphere is a complex, ever-evolving effort against a determined and resourceful adversary. Substantial efforts by U.S. Federal civilian agencies and State and local law enforcement agencies, supported by DOD, along with efforts by military and police forces from other nations, have made progress. However, demand for drugs remains a problem within our country, and the United States needs to continue its whole-of-government efforts to counter the flow of drugs coming north and the flow of weapons and money to the south. I view this as a major problem—where NORTHCOM can contribute to solving it, it should be an important part of the command’s mission. If confirmed, I will ensure NORTHCOM continues to work with interagency and international partners on all fronts to reduce the flow of narcotics into and within the NORTHCOM area of responsibility.

The geographic seam between SOUTHCOM and NORTHCOM is a key route for drugs to enter Mexico on their way to the United States. My understanding is that the two commands work closely together on this issue. Based on our collaboration in the aftermath of the Haiti earthquake, I have developed a close working relationship with General Doug Fraser, the Commander of SOUTHCOM. If confirmed, I fully expect to continue our work together to ensure a seamless effort across the border between the two areas of responsibility, to include further strengthening the relationships among Joint Interagency Task Force-South (JIATF–S), NORTHCOM’s Intelligence Directorate, and JTF–North.

Question. How are counterdrug operations coordinated across combatant command boundaries with PACOM?

Answer. Counterdrug operations, including those occurring on the boundaries with PACOM, are coordinated through sharing of intelligence information among combatant commands, interagency partners, the National Interdiction Centers, and PACOM’s Joint Interagency Task Force-West. I believe that synchronization among combatant commands is a critical ingredient of our Nation’s unity of effort in counterdrug operations. If confirmed, I will continue to nurture the relationship among NORTHCOM, PACOM, and SOUTHCOM regarding counter-drug information sharing and operations.

Question. If confirmed, what changes, if any, would you propose?

Answer. If confirmed, I look forward to working with the other combatant commanders and interagency partners NORTHCOM supports to identify and eliminate any operational seams to improve counterdrug operations.

Question. How would you recommend that the success of the Department’s counter-narcotics programs be measured?

Answer. I believe that success in counternarcotics is not easy to quantify. Traditional metrics, such as the price of drugs for sale on the street, are the product of many different factors, and their exclusive use could lead to false optimism or pessimism over our efforts. If confirmed, I intend to further explore this topic to determine whether there are useful input and output metrics that could be applied to NORTHCOM’s counternarcotics efforts.

Question. Do you believe that the current programs that the Department is pursuing are the most effective for the region, or should the Department’s efforts focus elsewhere?

Answer. DOD’s experience in countering insurgent and violent extremist networks is useful in countering drug trafficking networks, as all of these networks move people, material, money and information using clandestine methods. Accordingly, DOD’s contribution to interagency counternarcotics efforts is expanding. DOD normally takes a supporting role to the interagency in this arena. If confirmed, I look forward to forming my own assessment, and assisting DOD in determining which counternarcotics programs are most effective in the region to improve operational mission support to law enforcement and theater security cooperation efforts in combating these threats.

Question. Compared to other missions that you would be responsible for as Commander, NORTHCOM, if confirmed, where would you rank counter-narcotics in terms of its contribution to our national security and the ability of DOD to make a meaningful contribution?

Answer. NORTHCOM conducts missions to defend and secure the United States and its interests—these are no-fail missions. Drug trafficking directly affects our national security in several ways, including its corrosive effects within our society, violence along our border, and violence that severely impacts our neighbor and friend, Mexico. As such, I would rank contributing to counternarcotics efforts very high among NORTHCOM’s missions. If confirmed, and within appropriate limitations of
jurisdiction, sovereignty, and available resources, I will continue NORTHCOM’s efforts to support its domestic partner agencies and partner nations to address illicit narcotics and transnational threats to the Homeland.

Question. There has been a surge in drug-related violence in Mexico over the past year, which has increased the risk of cross-border violence into the United States. Much of the drug supply comes into Mexico across its southern border. The vast majority of Latin America, however, is in the SOUTHCOM AOR, so the security situation in Mexico is an example of the need for a well-coordinated effort between NORTHCOM and SOUTHCOM.

What is your vision of how SOUTHCOM and NORTHCOM could work together in a fully coordinated and seamless fashion with respect to Mexico and other security challenges?

Answer. While I believe the geographic boundary between NORTHCOM and SOUTHCOM is appropriately placed, it is absolutely critical that these two commands work effectively together on common security threats, including counter-narcotics. This will require: a strong partnership based on personal relationships; overall and theater security cooperation strategies that mesh closely together; deep information sharing enabled by quality liaison officers and modern technology; and a willingness to allow the opposite command to relate to partners in each other’s area of responsibility. If confirmed, I look forward to capitalizing on the excellent working relationship I developed with General Doug Fraser, the SOUTHCOM Commander, during operations in the aftermath of the Haiti earthquake.

Question. The United States and Mexico announced in 2007, the start of a multiyear, bilateral security agreement called the Mérida Initiative. This Initiative aims to combat drug trafficking and other criminal activity along the U.S.-Mexican border, as well as in Central America. The U.S.-Mexican border is viewed as especially important for U.S. counternarcotics efforts because Mexico is currently the primary point of entry for cocaine and other drug shipments smuggled into the United States.

What is your understanding of the Mérida Initiative as it relates to NORTHCOM?

Answer. It is my understanding that NORTHCOM plays a vital role in coordinating acquisition, contracting, and delivery of items provided through the Foreign Military Sales (FMS) and Foreign Military Financing (FMF) Programs within the auspices of the Mérida Initiative. These items improve the Mexican military’s ability to deploy rapid-reaction forces quickly in support of police operations against drug trafficking organizations, and to conduct maritime surveillance in an effort to deny the use of the eastern Pacific and western Caribbean to transnational criminal organizations, including drug traffickers and potential terrorists.

Additionally, NORTHCOM assists its Mexican military partners—while respecting Mexican sovereignty—with focused training, equipment, and related support intended to help reduce violence, weaken the drug trafficking organizations, ensure rule of law and respect for human rights, and set the conditions for the eventual operational takeover of the drug war by Mexican law enforcement authorities.

Question. What is your view of the appropriate role of DOD in countering transnational drug cartels and gangs?

Answer. Countering drug trafficking organizations is a transnational, trans-border effort that must be approached in a holistic, “whole-of-governments” manner. The DOD plays largely a supporting role in countering drug trafficking organizations and gangs by working closely with both domestic and international partners to counter these transnational threats.

In accordance with Federal statutes, NORTHCOM provides military support to Federal law enforcement agencies to assist in the identification and interdiction of transnational threats within and along the approaches to the United States. NORTHCOM also supports Federal law enforcement agencies through information collection, analysis, fusion, and sharing appropriate information.

Through its Theater Security Cooperation efforts, NORTHCOM is focused on building partner capability and capacity with Mexico and The Bahamas, and on enhancing coordination and interoperability with Canada, in order to develop and strengthen mutually beneficial partnerships to counter transnational drug trafficking organizations and gangs. NORTHCOM also works closely with its partner combatant commands through common strategies and information sharing in order to mutually enhance each command’s effectiveness in these efforts.

SECURITY RELATIONSHIPS WITH CANADA AND MEXICO

Question. The NORTHCOM area of responsibility includes the land areas of the United States, Canada, and Mexico. The binational NORAD Command ensures close cooperation between the United States and Canada on security matters.
NORTHCOM has been working with the Mexican military on security cooperation related to Mexico's efforts to counter drug trafficking and violence.

What is your assessment of the current security relationship between the United States and Canada?
Answer. I believe that our security relationship with Canada is excellent at all levels and in every Department of the U.S. Government. This relationship is characterized by extraordinary trust and confidence, evidenced by the long standing cooperation our two nations have enjoyed through the NORAD agreement. Canada has been an absolutely vital partner in the International Security Assistance Force's role in Afghanistan, conducting operations and making enormous sacrifices in some of the most challenging areas of that country. My understanding is that NORTHCOM also has a very strong relationship with its Canadian counterpart, Canada Command. If confirmed, I look forward to contributing to the success of this longstanding partnership.

Question. What is your assessment of the current security relationship between the United States and Mexico?
Answer. In my opinion, the current security relationship on a military-to-military level between the United States and Mexico is the best it has ever been. This was recently exemplified by the 30 March 2010 Mérida Initiative High-Level Consultative Group discussions held in Mexico City at the highest levels of our governments, which included the defense minister equivalents from both countries, as well as our Chairman of the Joint Chiefs of Staff. It is also reflected by military-to-military discussions that continue to grow in substance and importance, to include recently-held U.S.-Mexico Defense Bilateral Working Group discussions in Washington, DC.

Mexico is a critical partner that has demonstrated its commitment to combating drug trafficking organizations that affect the safety and security of North America. President Calderon and the Mexican military have been on the leading edge of a 3-year national effort to disrupt the drug trafficking organizations and curtail narco-violence in Mexico. NORTHCOM security cooperation activities continue to be a key and successful element of fostering a new era of U.S. Government-Government of Mexico collaboration.

Question. If confirmed, what would be your goals as Commander of NORTHCOM for improving security relations with Mexico, and how would you plan to achieve them?
Answer. If confirmed, I will continue the positive momentum NORTHCOM has established in this relationship. This will include: developing personal relationships with my counterparts informed by an understanding of their concerns; extending this level of trust downward through our respective chains of command; working to accelerate delivery of equipment under the Mérida initiative, as well as other capabilities; and continuing to provide training and information sharing requested by the Mexican authorities. I will capitalize on past and ongoing successes and look for new and innovative ways to build upon these achievements.

Question. What is your assessment of the security challenges to the United States posed by drug-related violence in Mexico?
Answer. In addition to the corrosive effects of drugs within our own cities, I believe the violence associated with drug trafficking in Mexico is a significant security challenge to the United States through its potential to spill over the border and by virtue of its severe negative impact on the internal security of a neighbor and friend. Mexican criminal organizations have been responsible for murders (including U.S. personnel who work in Mexico), kidnappings, extortion, human smuggling, arms and drug trafficking, and other violent activities.

It is my understanding that narco-violence increased in 2009, with some reports indicating 6,587 drug-related murders, up from 5,207 drug-related murders in 2008. Despite the increase in violence, President Calderon and the Mexican military are fighting back with notable successes, including the attempted apprehension of Arturo Beltran Leyva (Head of the Beltran Leyva Cartel, who was killed in the ensuing gun battle), the capture of his brother Carlos Beltran Leyva, and the arrest of Roberto Sánchez Arras, the one-time number three man in the Juárez Cartel. It is my belief that the U.S. Government should continue to provide security assistance to Mexico to build its capability and capacity to counter the violence that poses such a threat to their society.

NORTHCOM-STATE RELATIONS

Question. NORTHCOM has the primary military responsibility to provide defense support to civil authorities (DSCA) when directed by the President and the Secretary of Defense, including consequence management operations. Such military as-
Do you believe it is important for NORTHCOM to have an understanding of the emergency response capabilities and plans of the various States before a crisis arises, in order to optimize NORTHCOM's consequence management support to civil authorities?

Answer. Yes. I understand NORTHCOM already works collaboratively with the Federal Emergency Management Agency (FEMA), National Guard Bureau, and the States to anticipate DOD consequence management support to civil authorities and to coordinate potential requirements for effective consequence management. I have also observed that through NORTHCOM's Component Command, U.S. Army North, and their assigned Defense Coordinating Officers, that NORTHCOM works with the FEMA regional offices and States to improve relationships, information exchange, and mutual understanding. If confirmed, I look forward to participating in the Council of Governors meetings to further understand the States' capabilities and how DOD can best prepare to assist States in an emergency.

Question. If so, how would you plan to ensure that NORTHCOM has sufficient knowledge of State emergency response capabilities, including capabilities of National Guard units, and a good working relationship with State emergency response leaders?

Answer. If confirmed, I will ensure NORTHCOM continues its progress with FEMA, the National Guard Bureau, and the States in planning and integrating a whole-of-government approach to natural disaster response. In addition, if confirmed, I will examine NORTHCOM's staff substructure to determine if the command is organized optimally for this important mission area.

FORCE PROVISION FOR NORTHCOM

Question. NORTHCOM has the mission of conducting military operations for homeland defense and, when directed by the President or Secretary of Defense, for providing military assistance to civil authorities, including consequence management for natural disasters and CBRNE incidents. Yet NORTHCOM has relatively few military forces assigned to it on a permanent basis. What is your understanding of how forces are planned to be allocated to NORTHCOM for its full range of mission requirements, and the role that U.S. Joint Forces Command plays in that process?

Answer. It is my understanding that NORTHCOM's contingency plans and orders contain force requirements that are allocated by joint force providers. Forces are not normally identified or sourced until just prior to a planned event or impending incident, or immediately after a no-warning incident. The exceptions are the standing Execute Orders for CBRNE Consequence Management response forces and the Homeland Defense Quick Reaction Force/Rapid Response Force. Additionally, under the Defense Support of Civil Authorities Operations Standing Execute Order, the NORTHCOM Commander has the authority to place certain military capabilities on a 24-hour prepare-to-deploy order in advance of or in response to a contingency.

Question. If confirmed, how do you intend to ensure that NORTHCOM will have sufficient forces available to it, properly trained and equipped, to accomplish its assigned missions?

Answer. The Secretary of Defense allocates forces to Combatant Commands based on global requirements. The Service Chiefs, in accordance with their title 10 responsibilities, are responsible for providing combatant commanders trained and ready forces for employment within their respective areas of responsibility. If confirmed, I will ensure the Joint Staff and the joint force providers are aware of my force requirements, and that allocated forces are ready to perform their various missions required in supporting civil authorities and protecting the United States. I will maintain continuous liaison with joint force providers and the Services and, in order to promote speed-of-response, I will explore innovations that would enable pre-identification of the units that would be sourced to NORTHCOM in a contingency.

Question. If confirmed, how will you monitor the personnel, equipment and training readiness of U.S. military forces (Active and Reserve) for homeland defense mission-essential tasks in support of NORTHCOM's contingency plans, and for its DSCA missions?

Answer. As I understand it, NORTHCOM has the ability to track the readiness of title 10, title 32, and non-DOD capabilities of individual States throughout its area of responsibility using the Defense Readiness Reporting System (DRRS). NORTHCOM directly interfaces with the National Guard Bureau to obtain the readiness status of title 32 capabilities and is supporting the National Guard Bureau in establishing DRRS in every State. Moreover, if confirmed, I intend to work closely
with my Service and National Guard counterparts to personally observe, when possible and appropriate, the readiness of units that will be assigned Homeland Defense or DSCA missions.

NORTHCOM-DHS RELATIONSHIP

Question. The Department of Homeland Security is still a relatively new Federal agency, and is continuing to improve its ability to meet its homeland security missions. As the Department of Homeland Security improves and matures its homeland security capabilities, do you expect that will reduce the demands on NORTHCOM to provide DSCA?

Answer. This really depends on whether the combined capacity of civil and military resources in a particular mission area (such as counternarcotics or disaster response) is currently adequate. Where this is true, it can be viewed as a zero-sum situation in which additional Department of Homeland Security capability could reduce demands on NORTHCOM. However, there may be areas where our current capacity is inadequate, and increased Department of Homeland Security capacity will merely make additional progress towards buying down risk to a more acceptable level. If confirmed, I will collaborate with the Department of Homeland Security to understand how the various capacities mesh—both where savings may be realized and where additional capacity may be required.

Question. What do you consider to be the appropriate role for DOD and NORTHCOM’s vis-a-vis DHS and State authorities in identifying and validating the dual-use equipment and other requirements associated with defense and homeland security missions?

Answer. In accordance with the Secretary of Defense’s guidance, I believe the role of NORTHCOM is to coordinate with the Secretaries of the Military Departments, the Commander of SOCOM, the Commander of PACOM, and the Chief of the National Guard Bureau to identify critical dual-use equipment necessary for Active and Reserve component units and personnel to assist civil authorities in responses to natural disasters, acts of terrorism, and other man-made disasters as identified in the national planning scenarios. In accordance with my answer above, I believe it is also incumbent on NORTHCOM to coordinate with the Department of Homeland Security and State authorities as required to more fully understand equipment requirements in a resource-constrained environment.

RESPONSE TO CHRISTMAS DAY AIRCRAFT BOMB PLOT

Question. There has been considerable confusion about the events surrounding the attempted bombing of a commercial U.S. aircraft over Detroit on Christmas Day 2009. Do you believe that NORTHCOM or NORAD have any responsibility for apprehending, detaining, or interrogating a terrorist suspect who tries to destroy an aircraft in flight inside U.S. airspace? If so, what is that role?

Answer. Apprehending, detaining, or interrogating an individual alleged to have committed a criminal act within U.S. jurisdiction is a law enforcement function. NORAD conducts air defense operations as part of Operation Noble Eagle and would likely be involved operationally if needed, and both NORAD and NORTHCOM would remain alert for potential associated or follow-on attacks.

NATIONAL GUARD

Question. There is still debate about the role the National Guard should play in the Homeland. In an April 21, 2008 letter to the committee concerning the recommendations of the Commission on the National Guard and Reserves, Admiral Mullen, the Chairman of the Joint Chiefs of Staff, wrote that, “I have some concerns about the Commission’s ideas on enhancing the Defense Department’s role in the Homeland. While Reserve component civil support requirements are important, they should not be of equal importance to DOD combat responsibilities.” Do you agree with this view of Admiral Mullen?

Answer. Yes. Defending our country is the military’s primary duty, which is why all DOD forces, including the National Guard and Federal Reserves, are organized, trained, and equipped to fight our Nation’s wars. This is not to minimize the absolutely vital role the National Guard and Reserves play in civil support, and we must ensure these agile forces are adequately resourced and prepared for this mission.

Question. Do you believe that defending the Homeland or civil support should become the National Guard’s primary missions?

Answer. As a component of the Total Force, the National Guard has distinguished itself across full spectrum of DOD operations, both at home and abroad. Never has
this been more true than over the last 9 years of both conflict abroad and pressing missions at home. In my view, the National Guard should remain a full member of the Total Force. Their contribution to the success of DOD’s mission is too significant to be limited to just homeland defense and civil support. Moreover, to create additional force structure to execute the Federal missions currently being accomplished by the National Guard would be cost-prohibitive. In short, the Guard is providing exceptional service and flexibility to our Nation in its current status.

Question. What is the current status of the working relationship between NORTHCOM, the National Guard Bureau, and individual State National Guard headquarters?

Answer. My sense is that the working relationship among NORTHCOM, the National Guard Bureau, and individual States’ Guard headquarters has never been better and continues to improve. The robust National Guard presence within the NORTHCOM headquarters bears witness to this and fosters information sharing, collaborative planning, and Total Force mission execution that are paying dividends every day. If confirmed, I look forward to leveraging the excellent rapport I maintain with General Craig McKinley and other Guard leaders whom I have met in order to further advance this vital relationship.

Question. If confirmed, what type of liaison relationships for planning and operational purposes would you advocate between NORTHCOM, the Department of Homeland Security, Federal, State, and local first responders, and National Guard units under State authority?

Answer. As a former Joint Task Force Commander, I understand the value of strong, trusted relationships and their contribution to an organization’s success. If confirmed, I intend to enhance the existing liaison relationships that NORTHCOM currently already employs with these organizations by ensuring that liaison officers are empowered, motivated, and prepared to take all actions necessary to build relationships and understanding, conduct mutual planning, and remain prepared to transition seamlessly to cooperative execution. Where necessary, appropriate, and permitted by personnel resources, I will build new liaison relationships with key partners.

CBRNE RESPONSE CAPABILITIES

Question. NORTHCOM has two primary missions: Homeland Defense and DSCA, including preparation for and response to an incident or attack involving CBRNE materials or weapons, in the NORTHCOM area of responsibility.

If confirmed, how would you approach the challenge of ensuring adequate military forces, capabilities, and plans to respond to such incidents in support of civil authorities?

Answer. I believe the CBRNE Consequence Management (CM) mission in our homeland is a no-fail mission, and that forces assigned to this mission must be able to respond as required. NORTHCOM has developed detailed plans to support CBRNE CM in support of civil authorities. I understand the NORTHCOM CBRNE CM Response Forces are in transition and evolving into what is designed to be a robust and responsive force to provide faster life-saving capability and mitigate human suffering. If confirmed, I will work closely within DOD and with the National Guard and the States to ensure adequate forces are allocated to this mission and that they are properly trained, resourced, and exercised to maintain their readiness to respond when needed.

Question. There are currently a variety of organizations and units intended for CBRNE response and consequence management, including Joint Task Force-Civil Support (JTF–CS), the CBRNE Consequence Management Response Force (CCMRF), the U.S. Marine Corps Chemical-Biological Incident Response Force (CBIRF), National Guard Weapons of Mass Destruction Civil Support Teams (WMD–CSTs), and National Guard CBRNE Enhanced Response Force Package (CERFP) units.

If confirmed, how would you plan to manage this mix of capabilities to ensure the best possible response force to support civil authorities in the event of a CBRNE incident, and to avoid unnecessary duplication?

Answer. The military organizations designed to respond to a CBRNE CM incident are structured to provide a graduated response capable of handling small incidents, as well as large-scale incidents, in support of civil authorities. Some are Federal forces, while others are National Guard forces normally controlled by the State Governors. Each echeloned element is designed to respond under different timelines to build upon and integrate with the others to provide capability to civil authorities.

If confirmed, I intend to work closely with the National Guard Bureau and the States to ensure all forces established to accomplish this mission are properly
manned, trained, equipped to execute it, and that timelines and command and control relationships during execution are clearly understood and effective.

**Question.** What is your assessment of the ability of the CBRNE CCMRF, as currently constituted, to provide a significant capability to support Federal civil authorities in the event of a CBRNE incident?

**Answer.** It is my understanding that the two existing CCMRFs provide a responsive and flexible capability with federally-controlled forces that are trained, equipped, exercised, evaluated, and employed by NORTHCOM to respond to near-simultaneous incidents. I also understand that incremental modifications have been made to the CBRNE CCMRF concept—based on analysis and lessons learned from State- and national-level exercises—in order to improve its ability to provide comprehensive and self-sustaining support to first responders. I am also aware that DOD has determined that further improvements in CBRNE response capability are warranted to provide rapid response capability that is aligned within FEMA regions and responsive to State Governors.

**Question.** How would you assess the relative capabilities of a trained and equipped CCMRF to a trained and equipped National Guard CBRNE Enhanced Response Force Package (CERFP)?

**Answer.** It is my view that each of these forces present complementary capabilities that enhance our overall CBRNE Consequence Management response.

The CBRNE CCMRF is a relatively large force (4,000–4,500 personnel) that contains the required centralized capabilities to integrate with and support a Federal response under the National Response Framework. These capabilities include search and extraction, decontamination, air and ground casualty evacuation, mortuary affairs, information dissemination, communications, logistics, and a command and control structure to support integration of follow on forces.

CBRNE Enhanced Response Force Packages (CERFPs), under the control of State Governors, represent a much smaller (90–180 personnel), more agile and timely response force that is focused on regional support to provide security, triage, mass casualty and patient decontamination and stabilization.

When responding to a domestic event, both force elements provide a balanced approach by integrating and synchronizing the advantages of the National Guard CERFP and the robust Federal capability of the CCMRF.

**Question.** Do you believe that U.S. military forces providing DSCA in the event of CBRNE incidents should be under the command of the Commander, NORTHCOM?

**Answer.** In most cases, the incident will be managed at the State level with DOD in support. For all incidents, Federal forces would “lean forward”, as permitted under the National Response Framework, in order to monitor and assess CBRNE capabilities and provide additional support if requested. If title 10 forces do respond, I believe the Commander of NORTHCOM should maintain command and control of these forces in a “direct support” relationship aligned closely with the primary Federal agency and the affected State Governor(s) under the principle of unity of effort. In certain rare circumstances, the NORTHCOM Commander may be asked to assume overall command and control due to the nature or scope of an incident. If confirmed, I will ensure that Federal forces under my command are responsive under either command and control framework.

**WMD–CSTS AND CERFPs**

**Question.** There is now at least one National Guard Weapons of Mass Destruction-Civil Support Team (WMD–CST) in each of the 54 States and territories, and there are 17 National Guard CBRNE Enhanced Response Force Package (CERFP) units. Do you believe the WMD–CSTs and CERFPs are appropriately organized, sized, trained, and equipped to accomplish their assigned missions?

**Answer.** Yes, in my view, WMD–CSTs are appropriately organized, sized, trained and equipped to accomplish their assigned detection and analysis mission. WMD–CSTs are standardized forces and their training and readiness is overseen by NORTHCOM through its Army component, U.S. Army North.

I understand that there may be a need to improve CERFP organization, equipment standardization, and readiness. If confirmed, I will work with the National Guard Bureau to assist in any way to ensure that CERFPs are ready to accomplish their assigned mission in accordance with the CBRNE Enterprise identified in the 2010 Quadrennial Defense Review (QDR).

**Question.** If not, what changes do you believe are needed?

**Answer.** Today, I cannot say with certainty what changes are needed. However, if confirmed, I will quickly focus on CBRNE consequence management to do my part to ensure our nation has adequate response capability across the spectrum.
CBRNE CONSEQUENCE MANAGEMENT RESPONSE FORCE UNITS

Question. Several years ago, the Department decided to create three CBRNE CCMRF units to provide DSCA in the case of major CBRNE incidents in the United States requiring Federal consequence management. The recently released 2010 QDR proposed a significant restructuring of the CBRNE response force, from the 3 CCMRFs under DOD control, to 1 robust CCMRF, 2 military command and control units, and 10 future Homeland Response Forces (HRFs) within the National Guard and under the control of Governors in the 10 FEMA regions.

Do you believe the CCMRF concept, organization, and capability remain sound?

Answer. I believe the existing CCMRF concept was an important milestone toward achieving increased capability for this vital mission. The makeup of CBRNE response should inevitably represent a balance among speed, capability, resources, and ownership. Clearly, a robust Federal response to augment State and local responses is a vital component of this response. It is my sense that the restructuring directed by Secretary of Defense and outlined in the 2010 QDR represents an effort to refine this concept, and that DOD is committed to ensuring forces within the CBRNE CM Enterprise remain trained and ready, regardless of how they are organized. I understand NORTHCOM is actively working to fully outline this concept with DOD partners, especially the National Guard Bureau, and Federal interagency partners to ensure it is effectively employed.

Question. What is your assessment of the organization, capability, and potential effectiveness of the proposed HRFs in responding to a major CBRNE incident, as compared to the capability of the existing CCMRFs?

As I understand it, the intent of this decision is to rebalance the Nation’s CBRNE CM forces to better reflect the shared roles of the States and Federal government during a domestic event. As such, it appears to me that the HRFs were designed to provide a faster life-saving response than the existing CCMRFs, and to capitalize on the advantages of alignment with the FEMA regions, deeper regional knowledge, and State ownership.

That said, it remains important that a robust Federal response be prepared to augment the HRFs. This will be provided by a revised CCMRF that has 700 additional personnel and a more rapid response capability, along with two command and control CCMRFs that can coordinate responses to additional CBRNE events using general purpose forces.

It is my understanding that work is in progress at NORTHCOM, in collaboration with the requisite partners, on detailed implementation planning for this modified construct. If confirmed, I look forward to working with the National Guard Bureau and others to implement it properly, while at the same time closely monitoring training and readiness levels to ensure we provide the nation the strongest possible response capability.

Question. In your position as Director for Strategic Plans and Policy on the Joint Staff, were you involved in the debate and/or formulation of the HRF plan as outlined in the QDR?

Answer. No. Within the Joint Staff, the Force Structure, Resources, and Assessment Directorate partnered with the Office of the Secretary of Defense to lead the formulation of the HRF plan within the QDR effort. I was informed of my pending nomination for the position of Commander, NORTHCOM towards the end of the formulation and decision process, at which time I requested an information brief and attended two meetings as an observer.

Question. Do you believe it would be prudent to disestablish an existing CCMRF unit and eliminate its capability prior to having an equivalent alternative capability in place?

Answer. I do not believe it would be prudent to give up an existing capability prior to having an equivalent alternative capability in place.

Question. In order to ensure adequate defense support of civil authorities, do you believe the three CCMRFs, or any related units created from the proposed restructuring outlined in the QDR, should be Federal forces under the command of NORTHCOM?

Answer. In the new concept, Federal Restructured-CCMRF and the two smaller command and control elements created under the proposed restructuring outlined in the QDR should and will be under the command and control of the NORTHCOM Commander. State assets, such as the HRFs, CERFPs, and WMD–CSTs, will be under the command and control of the Governors through their Adjutants General, but could be Federalized under Title 10 if needed. If confirmed, I intend to work closely with the National Guard Bureau and the individual States to ensure command and control arrangements are clear and are exercised.
WESTERN HEMISPHERE INSTITUTE FOR SECURITY COOPERATION

Question. The Western Hemisphere Institute for Security Cooperation (WHINSEC), which replaced the School of the Americas in 2001, has the mission of contributing to theater cooperation activities through the education and training of students in the Western Hemisphere from Canada to Chile. If confirmed, you will be a member of the WHINSEC Board of Visitors.

What is the relationship between NORTHCOM and WHINSEC?

Answer. I understand that the National Defense Authorization Act of 2008 added the Commander of NORTHCOM to the WHINSEC Board of Visitors. The Board of Visitors reviews curricula to ensure compliance with U.S. laws, regulations, and policy goals, with an emphasis on human rights.

Question. In your view, does WHINSEC promote the national security interests of the United States in the Western Hemisphere?

Answer. It is my belief that WHINSEC is a strategic tool for international engagement that supports principles set forth in the Organization of American States Charter. WHINSEC’s professional education and training has a positive impact upon the 800–1,000 Latin American students in attendance annually from military, law enforcement and civilian institutions. I agree with the sense of Congress, as expressed in section 1084 of the National Defense Authorization Act for Fiscal Year 2010, that WHINSEC is building partner capacity that enhances regional and global security.

Question. In your view, how should NORTHCOM participate in command oversight and curriculum development?

Answer. As I understand it, NORTHCOM has an Academic Outreach and Human Rights Officer who is responsible for the hands-on oversight of WHINSEC from a NORTHCOM perspective and raises concerns to the commander as appropriate. If confirmed, I will evaluate the effectiveness of this arrangement to see if any changes are necessary, and will exercise personal oversight to ensure this process is effective.

Question. In your view, what more, if anything, does WHINSEC need to do to emphasize human rights in its curriculum?

Answer. I believe that human rights are an absolutely essential ingredient of the WHINSEC curriculum. If confirmed, I will examine this issue closely and determine if more emphasis is needed.

Question. In your view, how can WHINSEC improve its outreach efforts to individuals or groups interested in its activities, particularly those who have accused the school of contributing to human rights violations by former students?

Answer. After WHINSEC was activated, safeguards such as the Board of Visitors were put in place to ensure compliance with U.S. laws, regulations, and policy goals, with an emphasis on human rights. If confirmed, I will examine outreach efforts in order to determine whether they are effective, and to reassure these groups of NORTHCOM’s commitment to human rights within the WHINSEC curriculum.

Question. If confirmed, will you attend the WHINSEC Board of Visitor’s annual meeting?

Answer. If confirmed, I look forward to attending the Board of Visitors annual meeting—I will ensure that only a higher priority event requiring my presence would interfere with my attendance at the annual meeting.

INTELLIGENCE SHARING/NATIONAL COUNTERTERRORISM CENTER

Question. What is NORTHCOM’s role and involvement in developing intelligence assessments regarding terrorist threats?

Answer. It is my understanding that NORTHCOM develops all-source intelligence assessments of the transnational terrorist threat in order to provide warning and situational awareness in support of the missions of Homeland Defense, Defense Support of Civil Authorities, and Force Protection. NORTHCOM collaborates with all members of the Intelligence Community, other combatant commands, and the National Counterterrorism Center to ensure the command is able to anticipate potential responses to transnational terrorist threats as they develop.

Question. What intelligence agencies are involved in providing input to NORTHCOM’s staff for the development of intelligence assessments?

Answer. I understand that NORTHCOM develops intelligence assessments based on all-source intelligence derived from all 16 Intelligence Community members. This collaborative environment is fostered by a networked approach that allows NORTHCOM analysts to leverage relevant expertise throughout the Intelligence Community.

These collaborative relationships are created and maintained by a robust liaison program. National Agency Representatives from the Central Intelligence Agency,
National Security Agency, Federal Bureau of Investigation, National Geospatial-Intelligence Agency, Department of Homeland Security, the Service intelligence agencies, and the Defense Intelligence Agency are located within NORTHCOM.

Similarly, NORTHCOM liaison officers are located at the Department of Homeland Security, the Federal Bureau of Investigations, the National Counterterrorism Center (NCTC) the Canadian National Defence Headquarters in Ottawa.

**Question.** What is the current relationship between NORTHCOM and the NCTC?

**Answer.** It is my understanding that NORTHCOM has a strong relationship with the National Counterterrorism Center in a collaborative information-sharing environment. NORTHCOM routinely relies on the Center’s finished production and their collaborative tools, all of which is facilitated by having two full-time NORTHCOM personnel who are physically assigned to the Center as liaison officers.

**Question.** Does NORTHCOM have representatives located at the NCTC on a daily basis? If so, what are their functions and responsibilities? If not, why not?

**Answer.** Yes. NORTHCOM currently has two full-time liaison officers at the National Counterterrorism Center who facilitate the flow of information between NORTHCOM and the Center.

One liaison officer is assigned to the Defense Intelligence Unit, which is responsible for reviewing intelligence databases for information related to DOD equities. The other liaison officer is assigned to the Directorate of Strategic Operational Planning at the Center and ensures NORTHCOM is aware of and involved in community operational and contingency planning.

**Question.** Do you believe NORTHCOM representatives at NCTC have the access to intelligence needed to fully perform their functions?

**Answer.** Yes. It is my understanding that NORTHCOM liaison officers have access to all intelligence databases available to other Center analysts and are fully capable of performing their functions in support of the Center.

**Question.** How do posse comitatus, privacy restrictions, and other laws and regulations concerning the collection of intelligence within the United States, affect the way NORTHCOM receives and uses intelligence?

**Answer.** NORTHCOM accomplishes its intelligence mission within the framework of existing laws and policy; I understand NORTHCOM is vigilant in ensuring all intelligence activities conducted in support of its mission comply with intelligence oversight law and policy. If confirmed, I will ensure all intelligence activities conducted in support of NORTHCOM operations are reviewed by legal staff to ensure they are conducted in accordance with law and policy.

**BALLISTIC MISSILE DEFENSE**

**Question.** One of NORTHCOM’s missions is the defense of the United States against the threat of limited ballistic missile attack. The recently released Ballistic Missile Defense Review report stated as one of its policy priorities: “Before new capabilities are deployed, they must undergo testing that enables assessment under realistic conditions.” Do you agree that it is essential that our deployed ballistic missile defense systems are operationally effective?

**Answer.** Yes. In light of the growing threat from North Korea and Iran, both in numbers and sophistication, the capability to defend the Nation with an effective ballistic missile defense system is becoming increasingly important. The recently-announced Phased Adaptive Approach, a four-phase global approach, will provide a layered defense capability for the homeland, as well as for forward-deployed troops and allies.

**Question.** Do you agree that it is important to conduct operationally realistic flight tests to demonstrate the operational capability and reliability of the Ground-based Midcourse Defense (GMD) system?

**Answer.** Yes. Operationally realistic flight tests are one of the most important, and visible, ways of demonstrating the operational capability and reliability of the GMD system. I understand the NORTHCOM staff has worked closely with U.S. Strategic Command and the Missile Defense Agency in the formation of the Integrated Master Test Plan. This robust test plan lays the foundation for increasingly realistic operational flight tests over the next several years, and beyond.

**CRUISE MISSILE DEFENSE**

**Question.** NORTHCOM and NORAD have responsibilities for warning and defending the United States against airborne threats, including cruise missiles. Relative to cruise missile defense, what do you believe should be the relationship between the Joint Integrated Air and Missile Defense Organization (JIAMDO) of the Joint Staff, on the one hand, and NORTHCOM and NORAD, on the other hand?
Answer. I understand the JIAMDO has maintained a working partnership with NORAD since 1999 and NORTHCOM since its establishment in 2002. The JIAMDO has expanded its theater focus to include homeland air and cruise missile defense gaps, as well as ballistic missile defense gaps, through operational concept, architecture, and roadmap development efforts. The JIAMDO has a liaison office at NORAD and NORTHCOM to ensure daily coordination and collaboration. If confirmed, I look forward to building upon this relationship to enhance our homeland capabilities against the potential threat of a cruise missile attack.

Question. Relative to the full spectrum of threats to the United States, how would you assess the cruise missile threat to the United States and its territories?

Answer. I believe the overall cruise missile threat to the United States and its territories is currently low. While technically feasible, there are other means to use that are operationally easier for those who would harm us.

Question. If confirmed, what capabilities would you prioritize to address this threat?

Answer. While I believe the threat is currently low, continued efforts in Wide Area Surveillance of North America are needed to improve capabilities to address future capabilities. If confirmed, this will be a key area I will address, as well as a review of the NORAD and NORTHCOM Surveillance Gap Filler strategy. As I understand it, this strategy outlines the NORTHCOM plan to address air and maritime surveillance shortfalls through a family-of-systems approach to sensor development and improved information sharing of interagency sensors. Finally, through our intelligence resources, it is imperative that we remain alert to any game-changing evolution in capability that would raise the prominence of this threat.

CONTEMPTUAL AIR DEFENSE

Question. How has the continental air defense mission changed since the end of the Cold War and the events of September 11, 2001?

Answer. Prior to 11 September 2001, NORAD's air defense posture was aligned to counter external threats to North America. In response to the attacks on 11 September 2001, the command's mission was expanded to protect against domestic airborne threats originating within the United States and Canada.

Operation Noble Eagle began immediately after the September 11 attacks and continues today to protect and defend the airspace of the United States and Canada. NORAD implemented an improved air defense system by integrating radar, air patrols, surface-launched missiles, and control centers. This system also includes the capability to protect the National Capital Region from air attacks.

Question. Do you believe that current U.S. continental air defense capabilities are adequate to meet national security needs?

Answer. Yes. NORAD continues to adapt in an effort to counter the terrorist threat posed to the United States and Canada by maintaining a network of alert fighters, tankers, airborne early warning aircraft, and ground-based air defense assets. This capability, combined with improvements to surveillance and communication systems, as well as better coordination and information sharing with the interagency community, ensures NORAD provides air defense for the United States and Canada.

Question. If confirmed, what capabilities and programs would you prioritize to address any identified deficiencies?

Answer. If confirmed, I will examine NORAD's air defense capabilities with the goal of further improving the North American air surveillance picture not only for DOD, but also for our interagency partners—notably the National Capital Region Coordination Center and U.S. Customs and Border Protection. I understand that Homeland Air and Cruise Missile Defense, wide-area air surveillance, and refining intelligence sharing within the interagency community are critical to this effort. I will also work closely with the Services to ensure continuity of air sovereignty mission commensurate with postulated threats.

CONGRESSIONAL OVERSIGHT

Question. In order to exercise its legislative and oversight responsibilities, it is important that this committee and other appropriate committees of Congress are able to receive testimony, briefings, and other communications of information. Do you agree, if confirmed for this high position, to appear before this committee and other appropriate committees of Congress?

Answer. Yes.

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

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

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

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

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR JOHN MCCAIN

BORDER SECURITY

1. Senator McCain. Vice Admiral Winnefeld, what is your assessment of the current security situation along our southern border?
Admiral WINNEFELD. I view with concern the escalating violence along the Southwest border that in many cases is attributable to drug trafficking organizations. In addition to the corrosive effects of drugs within our own cities, I believe the violence associated with drug trafficking in Mexico is a significant security challenge to the United States through its potential to spill over the border and by virtue of its severe negative impact on the internal security of a neighbor and friend. As I mentioned in my hearing, if confirmed I plan to travel to the border region soon after taking command in order to more closely assess the situation.

2. Senator McCain. Vice Admiral Winnefeld, what is your view about the need for deployment of federally-funded national guardsmen along the southern border to assist and support civilian law enforcement agencies?
Admiral WINNEFELD. I believe that the National Guard has a place in support of civilian Federal, State, and local law enforcement agencies along the border. Indeed, over 300 title 32 forces from the 4 border States, specially trained in counterdrug activities, are currently deployed in support of the Department of Homeland Security (DHS), which is the lead Federal agency responsible for border security. I believe such deployments should be subject to the following principles: First, they should be undertaken only to the extent that the capacity of civilian agencies is exceeded by the security requirement or where the Guard can provide unique capability in support of civilian operations. In some cases, it may be necessary for the Department of Defense (DOD) forces to provide a bridge to increased DHS or local capacity. Second, such deployments should account for the impact they would have on support for U.S. troops that are engaged in combat overseas, as some of the capabilities that may contribute to border security are in short supply overseas. Third, I believe we need to be cautious about the perception of militarizing the border, though we should not allow this to prevent deployments required to guard against serious threats. Finally, these deployments should be made in response to a request from civilian agencies that is approved by the President or the Secretary of Defense. If confirmed, I will contribute to interagency assessments intended to assess the capacity and capabilities of civilian law enforcement and the suitability and magnitude of DOD contributions.

3. Senator McCain. Vice Admiral Winnefeld, what additional steps can U.S. Northern Command (NORTHCOM) take, in coordination with DHS, U.S. Southern Command (SOUTHCOM), and the Government of Mexico, to bring the drug-trade violence we are seeing on both sides of our southern border under control?
Admiral WINNEFELD. I believe that NORTHCOM has separate but complementary roles north and south of the border. It is my understanding that NORTHCOM is well-engaged with interagency partners, the Embassy Country Team, the Government of Mexico, and SOUTHCOM in evaluating ways the command can effectively support U.S. Government efforts to stem drug-trade related violence in our hemisphere. As one example, the command recently hosted and facilitated the Ciudad Juarez-El Paso Merida Planning Initiative from 22–26 February, 2010, with these
organizations. Those discussions, as well as coordination with these organizations on a daily basis, point to several additional steps that can be taken to stem the wave of violence that has gripped the border region.

If confirmed, I look forward to broadening and deepening the asymmetric warfare experience that we share with our domestic and Mexican partners. I will further pressurize our efforts in intelligence fusion and sharing, secure communications systems, biometrics equipment, night vision equipment, and accelerating the delivery of the helicopters and surveillance aircraft that are part of the Merida Initiative. I will seek ways to more effectively support DHS, the Department of Justice (DOJ), and other critical stakeholders in a whole-of-government approach to enhancing security along the southwest border. I will review current NORTHCOM initiatives, visit the Southwest border, listen to our Mexican partners, and assess how the command can support U.S. Government efforts to assist Mexico and other international partners in the region. Finally, I will work closely with SOUTHCOM to explore what additional steps we might take to enable the countries on Mexico's southern border to act more effectively to interdict drug traffic in that region.

LEGISLATIVE GAP IN RESERVE ACTIVATION AUTHORITY

4. Senator McCain. Vice Admiral Winnefeld, DOD currently lacks statutory authority to order Reserve personnel to involuntary Active Duty service for the purpose of providing civil support in response to a natural disaster. While such authority exists for terrorist attacks, proposals to give this legislative authority in response to a natural disaster has been opposed by State Governors, apparently due to a dispute about who will have operational control of Federal forces. What is your understanding of this problem and why have the States opposed ensuring that Federal Reserve Forces can be called up, if needed?

Admiral Winnefeld. Federal Reserve Forces have capabilities but only limited authorities to make important and timely contributions in support of local and State officials in response to domestic disasters. First, they may only be used for immediate, life-and-limb support when they are already on Active Duty status if/when a crisis occurs. Second, if they volunteer, they may be used only if there is also a request for assistance for title 10 support from another Federal agency. DOD is not authorized in any scenario to involuntarily mobilize Reserve Forces in response to a catastrophe or disaster.

State Governors, bound by their State constitutions to act as Commanders in Chief of their State forces, have been reluctant to support such authority until they better understand how such forces would be employed. Accordingly, they have taken the initial position that they must have command of all military forces (State and Federal) operating within their States. However, it is my understanding that constitutionally, the President of the United States, as Commander in Chief, cannot relinquish command of Federal forces.

To resolve this issue, OSD has proposed a concept to the Council of Governors addressing the command relationship as one of "direct support" using the principle of "unity of effort." Under this arrangement, which I fully support, Federal forces would "consult, coordinate with, and respond to State authorities" during a domestic disaster while maintaining existing command relationships. In this manner, Federal forces, including Federal Reserve Forces, would technically remain under the command of Federal authorities while responding directly to a Governor's needs. I have experienced this type of unity of effort relationship several times during my career, and it works. This concept is supported throughout the National Response Framework, which also emphasizes unity of effort vice unity of command.

5. Senator McCain. Vice Admiral Winnefeld, do you believe that title 10 Federal forces should be placed under the operational or tactical control of State Governors?

Admiral Winnefeld. No, I believe the Commander of NORTHCOM should maintain command and control of title 10 forces in a "direct support" relationship, remaining closely aligned with the primary Federal agency as well as coordinating closely with and remaining responsive to the affected State Governor(s) under the principle of unity of effort. I believe there is good balance in this construct. On the one hand, the President should maintain operational command of Federal forces for a variety of reasons. On the other hand, Federal forces should be very responsive to a Governor's needs in a crisis and be tightly aligned with the Adjutant General of the affected State. If confirmed, I intend to make it very clear to my State partners that we will act in support of a Governor's needs in time of crisis.
6. Senator McCain. Vice Admiral Winnefeld, what has been Secretary Gates’ position on this issue?

Admiral Winnefeld. Secretary Gates supports title 10 forces remaining under the Federal chain of command in accordance with subsection (b) of title 10, U.S.C. §162. Secretary Gates also reiterated at the Council of Governors meeting in February 2010 that he believes we can find a consensus approach that respects the Constitutional authorities of both the Governors and the President of the United States. I believe this is a sound approach and provides a positive way forward.

7. Senator McCain. Vice Admiral Winnefeld, do you believe NORTHCOM currently has sufficient authority to access Reserve component personnel and capabilities to fulfill your command’s mission?

Admiral Winnefeld. In terms of NORTHCOM’s primary mission of homeland defense, I believe DOD does, in fact, have sufficient authority to access Reserve component personnel and capabilities. However, in terms of NORTHCOM’s mission for Defense Support of Civil Authorities, I do not believe there is sufficient access to the Reserve component. In accordance with title 10, Army, Navy, Air Force, and Marine Federal reservists are only available for civil emergencies while in voluntary Inactive Duty for Training status.

The National Governors Association supported Congress’s rejection of a DOD-proposed statutory change that would have allowed the Secretary of Defense to order reservists to Active Duty to provide assistance when the response capabilities of Federal, State, and local civilian agencies are or could be exceeded. Under the knowledge possessed by the Governors at the time, I understand and am sympathetic to their rationale for not supporting this initiative. However, since then, OSD has begun working closely with the Governors to outline DOD’s concept of “direct support,” briefly described above. I am very hopeful that DOD can come to agreement with the Governors on this construct so that they will support a statutory change. I understand that the Council of Governors will discuss this issue further during their next meeting in June 2010, and if confirmed, I plan to attend that meeting to help forge a way ahead—and to make it clear to the Governors that I will be responsive to their needs in a crisis.

8. Senator McCain. Vice Admiral Winnefeld, would you recommend that we take action this legislative session to fix this problem?

Admiral Winnefeld. I believe that it is important to have the support of the Governors on solutions to this problem. I understand it was discussed extensively in the first Council of Governors meeting with the Secretary of Defense in February 2010. It is also my understanding that it will be further addressed at the next Council of Governors meeting in June 2010, and if confirmed, I plan to attend that meeting. With a better understanding of both DOD and the Governor’s concerns, appropriate actions for legislative session can be proposed—and I am hopeful that this will occur this year.

9. Senator McCain. Vice Admiral Winnefeld, what is the potential vulnerability if we do not take action?

Admiral Winnefeld. Certain DOD capabilities reside exclusively or in significant numbers in the Federal Reserve Forces, such as aerial spray, “Hurricane Hunter” weather reconnaissance, combat surgical hospitals, search and rescue, aeromedical evacuation, mortuary affairs, engineering and logistical support. Without this authority, these title 10 Federal Reserve Forces, which can be the most capable and closest unit to a disaster, cannot be involuntarily called forward to support a response, ultimately increasing costs and more importantly, risk to American lives. This is why it is critical that we forge a consensus solution as soon as possible and provide recommendations to Congress at that time.

J O I N T   R E S P O N S E S   T O   A T T A C K S

10. Senator McCain. Vice Admiral Winnefeld, how will NORTHCOM and CYBERCOM work together to support civil authorities in the event of a computer network attack on the Homeland?

Admiral Winnefeld. As I understand it, NORTHCOM has developed a very strong relationship with U.S. Strategic Command (STRATCOM). Once CYBERCOM stands up, I believe NORTHCOM will extend this relationship to CYBERCOM as well. Similar to the combatant commands, NORTHCOM is a routine consumer of the cyber security and information that STRATCOM and CYBERCOM will provide. In the event of an attack, NORTHCOM will work in a supported-supporting rela-
...tionship as designated by the Secretary of Defense to ensure the .mil domain is protected and that all available support is provided, as appropriate, to the owners of other domains.

11. Senator M. McCain. Vice Admiral Winnefeld, do roles and authorities exist to guide a joint response, if the Nation is attacked?

Admiral Winnefeld. The 2008 Unified Command Plan recognizes cyberspace as a warfighting domain, and NORTHCOM's mission set crosses all domains in order to defend, protect, and secure the United States and its interests against all threats, including cyber.

There are myriad authorities supporting Homeland Defense and Civil Support missions, as well as a joint response to cyber attack against the Nation. These include NORTHCOM authorities identified in title 10, as well as title 50, and the Unified Command Plan, Joint Strategic Capabilities Plan, Guidance for Employment of the Forces, and the National Response Framework. Additionally, there are a number of DOD policies and orders, contingency plans (to include NORTHCOM's Homeland Defense CONPLAN 3400), and Joint Staff-directed orders that guide a joint response. The authorities that are in place today for cyber center primarily on self-defense. If we had to act today in response to a cyber attack on critical national assets, the joint response would also be guided by the National Cyber Incident Response Plan. That said, I believe one of CYBERCOM's key roles will be to advise STRATCOM in recommending any adjustments to existing authorities required to better provide a joint response to an attack.

12. Senator M. McCain. Vice Admiral Winnefeld, with respect to other combatant commands, the Military Departments, and the many organizations within DOD, how will CYBERCOM function to ensure cyber operations are protected?

Admiral Winnefeld. As I understand it, CYBERCOM will have both supported and supporting cyber roles. As the supported command for defense of the Defense Information Networks, CYBERCOM will have the technical capability to conduct effective "defense in depth" protection of cyber operations and infrastructure that is common to all combatant commands. At the same time, as the supporting command, CYBERCOM will have the technical capability to provide information and awareness to enable its customers to effectively mitigate cyber threats to operations within their own areas of responsibility.

THREATS TO THE HOMELAND

13. Senator M. McCain. Vice Admiral Winnefeld, what do you consider to be the biggest threats to the Homeland?

Admiral Winnefeld. There are many potential threats to our Homeland, among which I would name five of particular concern. First, extremists who are directed, supported, or inspired by al Qaeda continue to plan terrorist attacks on our Homeland. Those attempting to obtain weapons of mass destruction pose the most consequential threat, while those pursuing smaller scale, hard-to-detect attacks using improvised explosive devices or conventional weapons represent the most likely threat. Second, I am concerned about the corrosive effect on our Nation's security of drug trafficking, including its associated violence, both inside Mexico and along our border. Third, the cyber threat to our information infrastructure is increasing in parallel with our growing reliance on the Internet. Fourth, North Korean and Iranian pursuit of nuclear weapons and the means to deliver them against our Homeland using long-range ballistic missiles or other means is a growing concern. Finally, the constant potential for a major natural disaster, which can produce damage far greater than most terrorist attacks, is something for which the NORTHCOM Commander must always be prepared.

14. Senator M. McCain. Vice Admiral Winnefeld, where do you assess the greatest vulnerabilities in our ability to defend the Homeland?

Admiral Winnefeld. I believe our greatest vulnerability remains extremist threats, who are determined and patient, will search for any path to produce violent events, and harbor no qualms about killing innocents to achieve their objectives. Our vulnerabilities to this threat derive from the immense array of potential targets within our Nation, the relative ease of entering a large and diverse country, and the extremists' intent to exploit the freedom of movement (and other important freedoms) we enjoy within our country.
15. Senator McCain. Vice Admiral Winnefeld, if confirmed, how will you address these vulnerabilities?

Admiral WINNEFELD. If confirmed, I will do everything in my power to ensure our Nation is prepared to handle the full spectrum of threats to our homeland. I will:

• Advocate the sense of urgency required to maintain vigilance against these threats;
• Nurture a culture that continuously challenges and improves our capability, particularly in the areas of information sharing with our partners and speed-of-response;
• Continue improvements to NORTHCOM's rigorous exercise program;
• Examine the NORTHCOM's homeland defense and civil support plans to ensure they address evolving threats and are tailored to need;
• Strengthen NORTHCOM’s relationships with its National Guard, interagency, State, local, tribal, and international partners to ensure the whole is greater than the sum of the parts;
• Work closely with the other COCOMs and service chiefs on issues of relevance to defending the Homeland;
• Remain cognizant of the health of our ballistic missile defense program; and
• Support a whole-of-government approach on both sides of our border with Mexico and strengthen Mexico's ability efforts against drug trafficking organizations.

INTEROPERABILITY WITH STATE AND LOCAL FIRST RESPONDERS

16. Senator McCain. Vice Admiral Winnefeld, a tragic lesson learned in the response to the attacks of September 11 was the inability of first responders to communicate amongst one another. Given the role DOD forces would assume in assisting State and local authorities in responding to large-scale incidents, the importance of these varying groups to communicate is vitally important if we are to avoid unnecessary miscommunication and risk. If confirmed, what steps will you take to ensure interoperability between title 10 forces and their civilian counterparts?

Admiral WINNEFELD. It is my belief that communications interoperability among all mission partners is a cornerstone of the Nation's response to disaster events. As I understand it, NORTHCOM has taken several initiatives to reduce miscommunication and ensure information sharing among our partners. NORTHCOM is a key participant in the Interagency Board for Equipment Standardization and Interoperability and the Federal Partnership for Interoperable Communications and, in concert with DHS and the National Guard Bureau, developed both the Strategic Operational Information Sharing Plan and the Deployable Communications Standards Publication. These efforts are critical in establishing interoperability protocols and standards for both communications systems and information exchange processes and will be used as the foundation for future procurement of DOD communications systems. I also believe it is important that we test these systems to ensure they function.

Further, NORTHCOM continues to partner with the National Guard Bureau and the Federal Emergency Management Agency on use and employment of our Deployable Cellular Systems and Incident Awareness and Assessment/Full Motion Video suites. These systems are designed for rapid employment to an incident to improve communications and shared situational awareness through augmented cellular phone services and video situational awareness to facilitate decisionmaking. In particular, mobile cellular capability can be used to mitigate commercial communications outages by providing cellular voice and data devices for key civilian leadership and agencies while at the same time providing radio communications interoperability among first responders and title 32/title 10 DOD forces.

17. Senator McCain. Vice Admiral Winnefeld, are you aware of any interoperability gaps between State and local first responders and title 10 forces?

Admiral WINNEFELD. I am not aware of any specific interoperability gaps forces among first responders and title 10 forces, but if confirmed I will look closely at interoperability in communications. As I understand it, NORTHCOM is dedicated to constantly improving processes and procedures to mitigate potential and unidentified gaps. For instance, since 2005 NORTHCOM has hosted an annual communications exercise solely designed to refine interoperable communications among National Guard, State, and local emergency management personnel and first responders. Last year's exercise conducted in Texas, Arizona, and South Carolina drew over 50 different participants from Federal, State, and local agencies.
Additionally, NORTHCOM is participating in efforts conducted by the Interagency Board and DHS’s Office of Interoperability and Compatibility to develop a Communications Unit Leader track under the National Incident Management System. This track is designed to train and certify communications personnel in typing incident scene communications requirements, standardizing processes and protocols, and providing a credentialing system to ensure equivalency among communications personnel.

**SHARING OF INFORMATION AND INTELLIGENCE BETWEEN AGENCIES**

18. Senator McCain. Vice Admiral Winnefeld, if confirmed, how will you seek to break down the barriers relating to intelligence collection and evaluation between agencies to ensure NORTHCOM has an accurate picture of potential threats?

Admiral WINNEFELD. I believe that persistent engagement and collaboration with our interagency partners is essential to ensure we are aware of and prepared to deal with emerging threats. To the maximum extent allowed by law and policy, we must strive for an “information push” rather than an “information pull” culture, as well as seek new ways of manipulating the information we do have in order to separate key threat signals from the noise. Often, this information is sensitive and closely held in law enforcement and/or intelligence channels. If confirmed, I will consistently articulate mission needs, particularly in the Force Protection and Defense Support of Civil Authorities arenas, while assuring the lead Federal agencies that we will safeguard their operational and investigative sensitivities. We must also pursue the activities in full compliance with Intelligence Oversight guidelines and ensure we maintain public trust in our ability to protect civil liberties. I will also strive to develop and maintain a solid and trusted set of relationships with the various intelligence agencies that includes as many liaison officers as feasible.

**RESTRUCTURING OF FEDERAL HOMELAND RESPONSE FORCES**

19. Senator McCain. Vice Admiral Winnefeld, the Quadrennial Defense Review (QDR) calls for a significant restructuring of the force packages NORTHCOM provides in support of civil authorities in the event of a large-scale disaster or attack. The proposal calls for the restructuring of one existing brigade-sized element, the elimination of another, and the creation of 10 smaller Homeland Response Forces (HRFs) to be spread throughout the 10 Federal Emergency Management Agency (FEMA) regions of the country. What are your views about this new approach?

Admiral WINNEFELD. As I understand it, the intent of this decision is to rebalance the Nation’s Chemical, Biological, Radiological, Nuclear, and high-yield Explosives (CBRNE) Consequence Management (CM) forces to better reflect the shared roles of the States and Federal Government during a domestic event. It also appears to me that the HRFs are designed to provide a faster life-saving response than the existing CBRNE CM Forces (CCMRFs) and to capitalize on the advantages of alignment with the FEMA regions, deeper regional knowledge, and State ownership.

That said, it remains important that a robust Federal response be prepared to augment the HRFs. This will be provided by a revised CCMRF that has 700 additional personnel and a more rapid response capability, along with two command and control CCMRFs that can coordinate responses to additional CBRNE events using general purpose forces.

It is my understanding that work is in progress at NORTHCOM, in collaboration with the requisite partners, on detailed implementation planning for this modified construct. If confirmed, I look forward to working with the National Guard Bureau and others to implement it properly, while at the same time closely monitoring training and readiness levels to ensure we provide the Nation the strongest possible response capability.

20. Senator McCain. Vice Admiral Winnefeld, are there any concerns about the apparent shift of authority of these forces from Federal control to that of the States, particularly given the potential for these forces to be moved and utilized across State lines?

Admiral WINNEFELD. Although work is ongoing to develop this new construct, I believe the various Federal and State response forces, under the National Response Framework, will be able to achieve unity of effort. My sense is that advance planning, gaming, exercising, and effective employment of the Emergency Management Assistance Compact will be important elements of a successful program. If confirmed, I intend to work closely with and through the National Guard Bureau to the States to ensure all forces established to accomplish this mission are properly
manned, trained, and equipped to execute it, and that timelines and command and control relationships during execution are clearly understood and effective.

QUESTIONS SUBMITTED BY SENATOR JAMES M. INHOFE

GUARD AND RESERVE IN NORTHERN COMMAND

21. Senator INHOFE. Vice Admiral Winnefeld, the integration of Active, Reserve, Guard, and interagency elements into your headquarters and the makeup of your subordinate units, makes NORTHCOM one of the most diverse agencies this Government has. As we all know, without our Guard and Reserve Forces, it would be impossible to conduct operations abroad while ensuring that our Homeland is secure and safe. I have legitimate concerns with respect to the impacts of Operation Enduring Freedom and Operation Iraqi Freedom rotations on our National Guard, as well as what I have been told to be the Air Force fighter reduction plan of 250 aircraft for the Air National Guard and its impacts on the 18 Air Sovereignty Alert site requirement. As I have been informed, this reduction in aircraft will reduce or cancel Operation Noble Eagle and the associated Combat Air Patrols (CAP) that were instituted post-September 11. What are your thoughts on the state of our National Guard and Reserves and their ability to provide support in times of crisis?

Admiral WINNEFELD. I believe our National Guard and Reserves have never been more capable than they are today; they are an amazingly versatile and battle-hardened force. From my point of view, they are critically important to NORTHCOM's mission, and their ability to provide support in times of crisis is solid and growing. If confirmed, I intend to develop a close relationship with the leadership of the Guard and Reserve—indeed, I already enjoy a superb relationship with the Chief, National Guard Bureau. While the Air Guard force structure resulting from the Air Force recapitalization plan remains to be seen, the professionals who employ this force will adapt with the demonstrated skill necessary to safeguard the Homeland.

22. Senator INHOFE. Vice Admiral Winnefeld, do you believe that NORTHCOM has the right mix of Active Duty, Reserve, and National Guard present within your command?

Admiral WINNEFELD. It seems to me that the NORTHCOM staff has a healthy mix of Active Duty and Reserve component—although, if confirmed, I will develop a more informed view. My understanding is that NORTHCOM has a Reserve component presence in every staff directorate HQs working alongside their Active Duty co-workers. In addition, I understand that the National Guard has made a significant investment in personnel assigned to NORTHCOM. In fact, NORTHCOM has the largest concentration of title 10 National Guard officers in a joint organization outside of the National Guard Bureau. I am aware that there are over 50 full-time Reserve component authorizations in NORTHCOM HQs, of which 45 are filled, which is about the same percentage that applies to the active component.

23. Senator INHOFE. Vice Admiral Winnefeld, can you confirm if there will be an Air Force fighter reduction in the Air National Guard? If so, what impact will it have on the 18 Air Sovereignty Alert sites and CAP requirements?

Admiral WINNEFELD. In my current position as Director of Strategic Plans and Policy for the Joint Staff, I am unable to confirm a reduction of the number of fighters in the Air National Guard; the balance between active and Guard force structure is a decision process led by the Department of the Air Force. However, if a reduction occurs, NORAD and NORTHCOM will work closely with the Air Force to ensure that the resulting force structure will still meet the requirements of Homeland Defense as directed under Operation Noble Eagle. I understand that the Air Force submitted to Congress, in response to National Defense Authorization Act language, a report that indicated that the 18 Air Sovereignty Alert sites would be unaffected by the fiscal year 2011 President’s budget position. If confirmed, I will work closely with the Air Force to ensure the Air Sovereignty Alert site configuration supports national guidance on Homeland Air Defense.

MISSILE DEFENSE

24. Senator INHOFE. Vice Admiral Winnefeld, I have spent a lot of time and energy with regards to missile defense and I am convinced that the current administration does not take the necessity of the program seriously. I believe we are underfunding missile defense programs and not driving the Missile Defense Agency (MDA) and others to develop a robust, layered, and integrated system of
ground-, sea-, and space-based radars and interceptors. I have specific concerns about the Phased Adaptive Approach:

- There is no map or plan showing the deployment of the system and how it will be integrated;
- While Aegis and our SM–3s are outstanding assets and vital to our national security, we do not have enough Aegis ships that are Ballistic Missile Defense (BMD) capable;
- I have been told we are having problems with the development of SM–3 1B which has taken expertise and focus away from 2A and 2B development, potentially pushing back the timeline;
- I am concerned about our ability to integrate all the radars we have into the existing BMD architecture which I have been told is limited looking out to the east (Iranian threat) as well as integrating Aegis with existing ground based radars;
- I am concerned there is not enough testing for our ground-based interceptors (GBIs) in Alaska and California nor are there enough missiles to ensure we can continue to test as well as maintain enough on status;
- I am concerned we have not tested the new kill vehicles that are being installed on our GBIs; and
- I am concerned that we are not moving forward on testing the two-stage GBI.

Every day there are open source reports of the efforts of North Korea and Iran, known enemies of the United States, to develop more advanced missiles and munitions with the intent to target the United States and our military forces. China and Russia continue their advancements as well, even as our President works to reduce our own capabilities and restrain our efforts to adequately defend the Nation. In short, our enemies are advancing their ability to reach out and hit us in a devastating way. What are your thoughts on whether we are assuming too much risk? If not, what can you tell me on how we are mitigating the known risk from those threats I have mentioned?

Admiral WINNEFELD. DOD spent considerable time during the recently concluded Ballistic Missile Defense Review (BMDR) assessing both evolving threats as well as our country’s current and projected capabilities over the next 10 years. I believe the Ground-based Midcourse Defense (GMD) system, as currently envisioned, will provide adequate defense against the evolving threat from North Korea and Iran, neither of which are currently capable of attacking the United States but which certainly possess the ambition to develop this capability. At the same time, DOD is placing additional emphasis on regional missile defense under the Phased Adaptive Approach (PAA) in order to pace the threat and provide assurance to our allies and partners. As such, we will be able to provide some measure of defense against medium and intermediate range missiles launched from the Middle East against our forces and our allies in Europe sooner than previously planned. Moreover, Homeland ballistic missile defense will benefit from this approach as soon as a surveillance radar becomes operational in southeastern Europe, which will provide earlier warning of an Iranian attack against the United States and increase the probability of success of GMD interception. In the longer term, when future interceptors such as the SM–3 Block IIB become operational, they could provide an additional layer of defense for the Homeland.

If confirmed, I will participate along with the other combatant commanders and service chiefs in the department’s ongoing analysis to ensure our future capability requirements and hedge strategies continue to stay ahead of the threat. I will also work to ensure that our systems are adequately tested and our operators properly trained to execute this important mission.

25. Senator INHOFE. Vice Admiral Winnefeld, have you looked at the recommendations on the development of either the three-stage or two-stage GBIs?

Admiral WINNEFELD. Yes, though if confirmed I will reinforce my knowledge of this program. My understanding is that the BMDR includes a hedge strategy that includes the continued development and assessment of a two-stage ground-based interceptor, including a test later this year. If confirmed, I will work closely with the MDA to explore the potential advantages of deploying a three-stage, two-stage mix of GBIs within the Homeland.

26. Senator INHOFE. Vice Admiral Winnefeld, what are your thoughts on a Third Site location on the east coast of the United States?

Admiral WINNEFELD. As a follow-on to the BMDR, the Department is examining how it will execute, operationally and programmatically, the tenets laid out in the
BMDR. I understand that as part of the ongoing analysis, the capabilities and deployment strategy being studied by NORTHCOM includes an east coast capability.

27. Senator INHOFE. Vice Admiral Winnefeld, on February 11, the Airborne Laser successfully intercepted a boosting ballistic missile—the first time a directed-energy system has destroyed such a target in any phase of flight. In a time of crisis, is there any plan to be able to use this aircraft to protect our Homeland?

Admiral WINNEFELD. The recent engagement test of the Airborne Laser demonstrated a unique capability in the area of BMD and is a pathfinder for future directed energy technologies. However, it is my understanding that due to the operational challenges associated with effectively employing this system against a real-world threat as opposed to the high cost of maintaining it, the program has been redesignated as a technology demonstration program and is therefore not part of the baseline BMD architecture.

28. Senator INHOFE. Vice Admiral Winnefeld, should we look into that?

Admiral WINNEFELD. It is my belief that during a time of crisis, the Department will seek to provide the combatant commands with the required capabilities to deter or, if necessary, defeat the threat.

QUESTIONS SUBMITTED BY SENATOR GEORGE S. LEMIEUX

BORDER SECURITY

29. Senator LEMIEUX. Vice Admiral Winnefeld, one of your areas of responsibility is the southwest border shared with Mexico. How secure are our southern borders and what recommendations do you have to stem the flow of humans and narcotics through them?

Admiral WINNEFELD. Illicit trafficking of drugs, arms, and bulk cash challenge the U.S. and Mexican Governments on both sides of the border. As such, my sense is that NORTHCOM has separate but complementary roles north and south of the border. Regarding the former, the command plays a supporting role to DHS, DOJ, and other critical stakeholders in a whole-of-government approach to enhancing security along the southwest border. If confirmed, I will look for ways to improve this support that are both effective and legal. Regarding the latter, given the Mexican military’s assigned role in the struggle against drug trafficking organizations, NORTHCOM plays a vital role in enhancing the Mexican military’s capability and capacity, which I would seek to enhance. If confirmed, I look forward to reviewing current NORTHCOM initiatives, visiting the Southwest border, listening to our Mexican partners, and assessing how best the command can support U.S. Government efforts to assist Mexico and other international partners in the region.

BALLISTIC MISSILE DEFENSE

30. Senator LEMIEUX. Vice Admiral Winnefeld, what is your assessment of America’s current ballistic missile defense capabilities and in what areas would you like to see further development?

Admiral WINNEFELD. It is my belief that the GMD system adequately addresses the potential rogue threats we face today. The MDA’s evolutionary development of the GMD system continues to demonstrate technology enhancements that will enable us to defeat the evolving threats from long-range missiles under development by North Korea and Iran.

Meanwhile, the newly-adopted Phased Adaptive Approach (PAA) in Europe, intended to pace the threat by providing defense against medium and intermediate ballistic missiles coming from the Middle East much sooner, should also provide deployable, agile, and tailororable defensive capabilities to enhance defense of the Homeland. For example, in the near term, a PAA surveillance radar in southeastern Europe will provide earlier warning of a ballistic missile attack from Iran, and thus provide the GMD system with a higher probability of intercepting such a threat. In the long term, when future interceptors such as the SM–3 Block IIB become operational, they will provide an additional layer of defense.

As for areas requiring further development, I believe we must continue developing our space-based sensor capabilities in order to attain a birth-to-death tracking and engagement capability and we need to continue moving into a net-centric integrated architecture to enable service, agency, and potentially allied systems integration to facilitate data sharing, situational awareness and coordinated engagement capabilities.
EGUARDIAN SYSTEM

31. Senator Lemieux. Vice Admiral Winnefeld, the eGuardian system is an unclassified system, that once implemented, will help DOD and law enforcement identify suspicious activity and hopefully preempt a terrorist attack. How close are we to implementing this system?

Admiral Winnefeld. As I understand it, the Under Secretary of Defense for Policy will establish a plan and issue policy and procedures for the implementation of the eGuardian system no later than June 30, 2010. The Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs estimates that the fielding and implementation of eGuardian will begin in September 2010. Implementation in the NORTHCOM area of responsibility will be scheduled in four phases, followed by a fifth phase for the other Geographical Combatant Commands. Each implementation phase will involve all Service components, Services, and agencies and each phase will require 60-to-90 days for completion.

CYBER ATTACKS

32. Senator Lemieux. Vice Admiral Winnefeld, in your opinion, how should government-sanctioned Chinese cyber penetrations of American companies be categorized? Is it an act of war, a violation of international law, or something else?

Admiral Winnefeld. It is my belief that, depending on the circumstances, a cyber intrusion into a privately owned network could constitute one of the following: a violation of international law, a violation of domestic law, espionage, a violation of a State’s sovereignty, or an act of trespass. In my opinion, such an intrusion would only be an act of war if it were conducted by an identifiable adversary and included demonstrated intent, planning, and execution, leading to actual destruction of our infrastructure or our financial system.

QUESTIONS SUBMITTED BY SENATOR SUSAN COLLINS

HOMELAND RESPONSE

33. Senator Collins. Vice Admiral Winnefeld, in the recently released QDR, the Pentagon announced plans to develop HRFs in each of the 10 FEMA regions. These units would respond to domestic incidents involving weapons of mass destruction, or other catastrophic disasters. How do you envision the HRF’s coordinating, planning, training, and exercising with the FEMA regional offices?

Admiral Winnefeld. NORTHCOM is working closely with the National Guard Bureau and other mission partners to develop integrated plans for employment of the HRFs. The HRF concept aligns the HRFs with the 10 FEMA regions and tasks them with coordinating regionally focused military planning, training, exercises, and other efforts to support unity of effort across Federal, State, and local responses. As such, I would expect a close coordinating relationship between the HRFs and the FEMA regional offices, as well as with the NORTHCOM Defense Coordinating Officer within each FEMA region. If confirmed, I look forward to working together with the National Guard Bureau as the HRF capability stands up.

34. Senator Collins. Vice Admiral Winnefeld, one of the most effective ways to enhance our National preparedness is to develop coordinated and detailed plans for preventing and responding to disasters before they occur. DOD has unique planning capabilities that can be brought to bear to assist in these efforts. How can the Pentagon, and NORTHCOM specifically, more effectively leverage its planning expertise to assist DHS and other Federal agencies in planning for catastrophic natural disasters or terrorist attacks?


• NORTHCOM planners participate, in coordination with OSD and the Joint Staff, in all levels of planning with DHS and FEMA, from mission analysis to approved and published Federal plans.
• NORTHCOM, when requested by DHS/FEMA, routinely sends planners to assist in planning efforts.
• NORTHCOM attends and hosts planning conferences with its mission partners to coordinate and provide planning assistance.
NORTHCOM shares its plans with critical mission partners, including Federal agencies. The National Security Staff is leading the development of a National Preparedness Presidential Policy Directive that will supersede HSPD–8 (including Annex I) and will implement a new planning system. If confirmed, I will ensure NORTHCOM continues to provide planning expertise on the development of Federal interagency plans, attend and host planner-related events, and continue to share plans and information to foster a closer working relationship with Federal partners.

[The nomination reference of VADM James A. Winnefeld, Jr., USN, follows:]

NOMINATION REFERENCE AND REPORT

AS IN EXECUTIVE SESSION,
SENATE OF THE UNITED STATES,

Ordered, That the following nomination be referred to the Committee on Armed Services:
The following named officer for appointment in the U.S. Navy to the grade indicated while assigned to a position of importance and responsibility under title 10, U.S.C., section 601:

To be Admiral.
VADM James A. Winnefeld, Jr., 5212.

[The biographical sketch of VADM James A. Winnefeld, Jr., USN, which was transmitted to the committee at the time the nomination was referred, follows:]

DEPARTMENT OF THE NAVY,
2000 NAVY PENTAGON,
Washington, DC, October 29, 2009.

Hon. CARL LEVIN, Chairman,
Committee on Armed Services,
U.S. Senate,
Washington, DC.

DEAR MR. CHAIRMAN: The President, under the provisions of section 601, title 10, U.S.C., has submitted to the Senate the nomination of Vice Admiral James A. Winnefeld, Jr., U.S. Navy, for appointment to the grade of admiral.

Vice Admiral Winnefeld is presently serving as Director, Strategic Plans and Policy, J–5, Joint Staff; Senior Member, U.S. Delegation to the United Nations Military Staff Committee. He will be assigned as Commander, Northern Command/Commander, North American Aerospace Defense Command. He is 53 years of age.

This action will not result in the Navy exceeding the number of authorized four-star positions.

For the information of the committee, I am enclosing a career resume on Vice Admiral Winnefeld which includes a summary of his joint duty assignments.

Most respectfully,

R.S. ERSKINE,
Director, Flag Officer
Management and Distribution.

cc:
Hon. John McCain, Ranking Member,
Committee on Armed Services,
U.S. Senate,
Washington, DC.

TRANSCRIPT OF NAVAL SERVICE FOR VADM JAMES ALEXANDER WINNEFELD, JR., USN

24 April 1956 Born in Coronado, CA
07 June 1978 Ensign
07 June 1980 Lieutenant (junior grade)
**Assignments and duties:**

<table>
<thead>
<tr>
<th>Date From</th>
<th>Date To</th>
<th>Position and Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 1978</td>
<td>Nov. 1978</td>
<td>Naval Station, Annapolis, MD (Division Officer)</td>
</tr>
<tr>
<td>Nov. 1978</td>
<td>Apr. 1979</td>
<td>Naval Aviation Schools Command, Pensacola, FL (DUINS)</td>
</tr>
<tr>
<td>Apr. 1979</td>
<td>June 1979</td>
<td>Training Squadron SIX (Student)</td>
</tr>
<tr>
<td>June 1979</td>
<td>Dec. 1979</td>
<td>Naval Aviation Schools Command, Pensacola, FL (DUINS)</td>
</tr>
<tr>
<td>Dec. 1979</td>
<td>May 1980</td>
<td>Training Squadron TWO TWO (Student)</td>
</tr>
<tr>
<td>Apr. 1981</td>
<td>Nov. 1983</td>
<td>Fighter Squadron TWO FOUR (Power Plants Branch Officer)</td>
</tr>
<tr>
<td>Nov. 1983</td>
<td>Jan. 1987</td>
<td>Naval Fighter Weapons School, San Diego, CA (Quality Assurance Officer)</td>
</tr>
<tr>
<td>Jan. 1987</td>
<td>Apr. 1987</td>
<td>Fighter Squadron ONE TWO FOUR (Replacement Naval Aviator)</td>
</tr>
<tr>
<td>Apr. 1987</td>
<td>Jan. 1990</td>
<td>Fighter Squadron ONE (Operations Officer)</td>
</tr>
<tr>
<td>Feb. 1990</td>
<td>July 1991</td>
<td>Joint Staff (Senior Aide-De-Camp to the Chairman of the Joint Chiefs of Staff)</td>
</tr>
<tr>
<td>July 1991</td>
<td>Aug. 1992</td>
<td>Joint Staff (Action Officer, EUCOM/CENTCOM Branch, J3)</td>
</tr>
<tr>
<td>Aug. 1992</td>
<td>Jan. 1993</td>
<td>Fighter Squadron ONE TWO FOUR (Student)</td>
</tr>
<tr>
<td>Jan. 1993</td>
<td>Apr. 1994</td>
<td>XO, Fighter Squadron TWO ONE ONE</td>
</tr>
<tr>
<td>Apr. 1994</td>
<td>Mar. 1995</td>
<td>CO, Fighter Squadron TWO ONE ONE</td>
</tr>
<tr>
<td>Mar. 1995</td>
<td>Feb. 1996</td>
<td>Naval Nuclear Power Training Command, Orlando, FL (Student)</td>
</tr>
<tr>
<td>Feb. 1996</td>
<td>Mar. 1996</td>
<td>Prospective Executive Officer, USS John C. Stennis (CVN 74)</td>
</tr>
<tr>
<td>Mar. 1996</td>
<td>Aug. 1996</td>
<td>Naval Reactors, Department of Energy, Washington, DC (Student)</td>
</tr>
<tr>
<td>Aug. 1996</td>
<td>May 1998</td>
<td>XO, USS John C Stennis (CVN 74)</td>
</tr>
<tr>
<td>May 1998</td>
<td>Feb. 2000</td>
<td>CO, USS Cleveland (LPD 7)</td>
</tr>
<tr>
<td>Mar. 2002</td>
<td>July 2003</td>
<td>Office of the Vice Chief of Naval Operations (Executive Assistant)</td>
</tr>
<tr>
<td>July 2003</td>
<td>Dec. 2004</td>
<td>Commander, U.S. Atlantic Fleet (Director, Warfare Programs and Readiness) (ND)</td>
</tr>
<tr>
<td>Dec. 2004</td>
<td>June 2006</td>
<td>Commander, Carrier Strike Group TWO</td>
</tr>
<tr>
<td>June 2006</td>
<td>Aug. 2007</td>
<td>Commander, U.S. Joint Forces Command (Director of Joint Innovation and Experimentation, J9)</td>
</tr>
<tr>
<td>Aug. 2007</td>
<td>To date</td>
<td>Commander, SIXTH Fleet/Commander, Joint Headquarters Lisbon</td>
</tr>
<tr>
<td>Sep. 2007</td>
<td>Aug. 2008</td>
<td>Joint Staff (Director, Strategic Plans and Policy) (JS)/Senior Member, U.S. Delegation to the United Nations Military Staff Committee</td>
</tr>
</tbody>
</table>

**Medals and awards:**
- Defense Superior Service Medal
- Legion of Merit with two Gold Stars
- Bronze Star Medal
- Defense Meritorious Service Medal
- Meritorious Service Medal
- Air Medal with First Strike/Flight Award
- Navy and Marine Corps Commendation Medal with one Gold Star
- Joint Service Achievement Medal
- Navy and Marine Corps Achievement Medal
- Joint Meritorious Unit Award
- Navy Unit Commendation with one Bronze Star
- Navy “E” Ribbon with “E” Device
- National Defense Service Medal with one Bronze Star
- Armed Forces Expeditionary Medal with two Bronze Stars
- Southwest Asia Service Medal with one Bronze Star
- Global War on Terrorism Expeditionary Medal
- Global War on Terrorism Service Medal
- Sea Service Deployment Ribbon with one Silver Star and one Bronze Star
- Expert Pistol Shot Medal

**Special qualifications:**
- BS (Aerospace Engineering) Georgia Institute of Technology, 1978
- Designated Naval Aviator, 1980
- Capstone, 2004–3
Personal data:
Wife: Mary Alice Werner of Menomonie, WI

Summary of joint duty assignments:

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Dates</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joint Staff (Action Officer, EUCOM/CENTCOM Branch, J3)</td>
<td>Feb. 90–July 91</td>
<td>LCDR</td>
</tr>
<tr>
<td>Joint Staff (Senior Aide-De-Camp to the Chairman of the Joint Chiefs of Staff)</td>
<td>July 91–Aug. 92</td>
<td>CDR</td>
</tr>
<tr>
<td>Commander, SIXTH Fleet/Commander, Striking and Support Forces NATO/Deputy Commander, U.S. Naval Forces Europe/Commander, Joint Headquarters Lisbon</td>
<td>June 06–Aug. 07</td>
<td>RADM</td>
</tr>
<tr>
<td>Joint Staff (Director, Strategic Plans and Policy) (SJS/Senior Member, U.S. Delegation to the United Nations Military Staff Committee)</td>
<td>Sep. 07–Aug. 08</td>
<td>VADM</td>
</tr>
<tr>
<td></td>
<td>Aug. 08–To date</td>
<td>VADM</td>
</tr>
</tbody>
</table>

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

UNITED STATES SENATE
COMMITTEE ON ARMED SERVICES

Room SR–228
Washington, DC 20510–6050
(202) 224–3871

COMMITTEE ON ARMED SERVICES FORM

BIOGRAPHICAL AND FINANCIAL INFORMATION REQUESTED OF NOMINEES

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

PART A—BIOGRAPHICAL INFORMATION

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

1. Name: (Include any former names used.)
   James A. Winnefeld, Jr. (nickname: Sandy)

2. Position to which nominated:

3. Date of nomination:
   20 January 2010.

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

5. Date and place of birth:
   24 April 1956; Coronado, CA.

6. Marital Status: (Include maiden name of wife or husband’s name.)
   Married to the former Mary Alice Werner.
7. **Names and ages of children:**
   James A. Winnefeld III, age 13; Jonathan J. Winnefeld, age 11.

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

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

10. **Memberships:** List all memberships and offices currently held in professional, fraternal, scholarly, civic, business, charitable, and other organizations.
    Member (otherwise referred to as a Trustee) of U.S. Naval Academy Foundation: Athletic and Scholarship Programs (a nonprofit organization).

11. **Honors and awards:** List all scholarships, fellowships, honorary society memberships, and any other special recognitions for outstanding service or achievements other than those listed on the service record extract provided to the committee by the executive branch.
    Member of the Academy of Distinguished Engineering Alumni, Georgia Institute of Technology.

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

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

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

**SIGNATURE AND DATE**

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

JAMES A. WINNEFELD, JR.

This 29th day of October, 2009.

[The nomination of VADM James A. Winnefeld, Jr., USN, was reported to the Senate by Chairman Levin on May 5, 2010, with the recommendation that the nomination be confirmed. The nomination was confirmed by the Senate on May 7, 2010.]

[Prepared questions submitted to LTG Keith B. Alexander, USA, by Chairman Levin prior to the hearing with answers supplied follow:]

**QUESTIONS AND RESPONSES**

**DEFENSE REFORMS**

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

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

Answer. The integration of joint capabilities under the Goldwater-Nichols Act has been a remarkable achievement. Our military forces are more interoperable today than they ever have been in our Nation's history. I do not see a need to modify the Goldwater-Nichols Act at this time.

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

DUTIES

Question. What is your understanding of the duties and functions of the Commander, U.S. Cyber Command?

Answer. In accordance with Secretary of Defense guidance of June 23, 2009, the Commander, U.S. Cyber Command is responsible for executing the specified cyber-space missions detailed in Section 18d(3) of the Unified Command Plan (UCP) as delegated by the Commander, U.S. Strategic Command to secure our freedom of action in cyber space and mitigate the risks to our national security that come from our dependence on cyberspace and the associated threats and vulnerabilities. Subject to the Commander, U.S. Strategic Command, delegation and in coordination with mission partners, specific missions include: integrating cyberspace operations and synchronizing warfighting effects across the global security environment; providing support to civil authorities and international partners; directing global information grid operations and defense; executing full-spectrum military cyberspace operations; serving as the focal point for deconfliction of the Department of Defense (DOD) offensive cyberspace operations; providing improved shared situational awareness of cyberspace operations, including indications and warning; and providing military representation to U.S. national agencies, U.S. commercial agencies, and international agencies for cyberspace matters.

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

Answer. I am deeply honored that the President nominated me to be the first Commander of U.S. Cyber Command. Over the past 3 decades, I have served in a wide variety of Joint and Army positions, including 15 years in command, that have prepared me well for the challenges ahead if confirmed by the U.S. Senate.

First, I have 35 years in the profession of arms, serving in various command, staff and intelligence positions in the military. I have served as the Deputy Chief of Staff of Intelligence, Headquarters, Department of the Army; Commanding General of the U.S. Army Intelligence and Security Command; Director of Intelligence, U.S. Central Command; and Deputy Director for Requirements, Capabilities, Assessments, and Doctrine, J–2, for the Joint Chiefs of Staff.

Second, my experiences and knowledge gained over the last 4½ years serving as Director, National Security Agency (NSA), Chief, Central Security Service and Commander, Joint Functional Component Command-Network Warfare (JFCC–NW) have been instrumental in preparing me for the challenges of this new complex warfighting domain that is cyberspace. NSA’s cryptologic work in SIGINT/Computer Network Exploitation, Information Assurance and Network Threat Operations is second to none and foundational to our future success in the cyber domain. I have personally championed NSA’s work and learned a great deal from the outstanding professionals at NSA/CSS. Over the last 4½ years, I have also forged important partnerships with both our allies and with industry to strengthen the defense of our collective networks. Furthermore, my assignment as the Commander, JFCC–NW, including operational control over Joint Task Force-Global Network Operations (JTF–GNO) for the past 18 months, has provided me with the experience, particularly in the realm of deliberate and crisis action planning, to ensure the effective execution of cyberspace responsibilities as directed by the Secretary of Defense through Commander, U.S. Strategic Command.

Finally, I believe my academic background has intellectually prepared me for the challenges of high-level command and complex environments. I have Masters of Science degrees in Business Administration, Systems Technology (Electronic Warfare) and Physics, as well as National Security Strategy.

Question. If confirmed as the Commander of U.S. Cyber Command, would you have command of or exercise operational control of the Defense Information Systems Agency’s (DISA) and Military Services’ communications networks?

Answer. If confirmed as Commander, U.S. Cyber Command, I will be responsible for directing the operation and defense of DOD’s military information networks as specified in the UCP and as delegated by Commander, U.S. Strategic Command. I
will execute this mission through each of the Service Network Operations and Security Centers. I will not exercise command or operational control over the DISA communications networks. DISA will continue to be responsible for acquiring, engineering and provisioning enterprise infrastructure to assure the availability of military information networks. As a Combat Support Agency, DISA will maintain a close working relationship with U.S. Cyber Command, providing expertise on the networks, communications and computing infrastructure operated by DISA through both a DISA Field Office and a DISA Support Element.

**Question.** As a career intelligence officer, what experience do you have that qualifies you to command these networks and to command military forces and military operations?

**Answer.** Answer provided in the classified supplement.

**Question.** Do you believe that there are any steps that you need to take to enhance your expertise to perform the duties of the Commander, U.S. Cyber Command?

**Answer.** I fundamentally believe that there is always something to be learned to enhance my expertise in this very complex and dynamically changing domain. If confirmed, I will engage with combatant commanders to understand better how U.S. Cyber Command can best support and help meet their operational missions. Additionally, I would engage with key officials and personnel within the Executive and Legislative branches of the U.S. Government, senior military leaders, and leaders throughout the Intelligence Community in order to identify, assess, and mitigate the cyber threats we face.

**Question.** Is there a precedent for a career intelligence officer to serve as a combatant commander?

**Answer.** I know of no career intelligence officers who have previously served as either a combatant or subunified commander. However, two former Directors of NSA, General Lew Allen and Admiral Noel Gayler, served with great distinction as the Chief of Staff, U.S. Air Force and Commander, U.S. Pacific Command, respectively.

### RELATIONSHIPS

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

#### The Secretary of Defense.

**Answer.** Pursuant to title 10, U.S.C., section 164, subject to the direction of the President, the Commander, U.S. Strategic Command, performs duties under the authority, direction, and control of the Secretary of Defense and is directly responsible to the Secretary for the preparedness of the command to carry out missions assigned to the command. As a subunified command under the authority, direction, and control of the Commander, U.S. Strategic Command, U.S. Cyber Command will be directly responsible to the Secretary of Defense through the Commander, U.S. Strategic Command. If confirmed, I will work closely with the Secretary in coordination with Commander, U.S. Strategic Command, on matters of strategic importance.

#### The Deputy Secretary of Defense.

**Answer.** In accordance with title 10, U.S.C., section 132, the Deputy Secretary of Defense will perform such duties and exercise powers prescribed by the Secretary of Defense. The Deputy Secretary of Defense will act for the Secretary of Defense when the Secretary is disabled or the office is vacant. If confirmed, I will work closely with the Deputy Secretary, in coordination with Commander, U.S. Strategic Command, on matters of strategic importance.

#### The Director of National Intelligence.

**Answer.** The Intelligence Reform and Terrorist Prevention Act of 2004 established the Director of National Intelligence to act as the head of the Intelligence Community, principal advisor to the President, National Security Council, and Homeland Security Council on intelligence matters pertaining to national security, and to oversee and direct the implementation of the National Intelligence Program. Pursuant to title 50, U.S.C., section 403, subject to the authority, direction, and control of the President, the Director of National Intelligence is responsible to coordinate national intelligence priorities and to facilitate information sharing among the Intelligence Community. If confirmed, I will work closely with the Commander, U.S. Strategic Command and through the Secretary of Defense to coordinate and exchange information with the Director of National Intelligence as needed to ensure unified effort
and the leveraging of available synergies within the Intelligence Community to support matters of national security.

*Question.* The Under Secretary of Defense for Policy.

*Answer.* Title 10, U.S.C. and current DOD directives establish the Under Secretaries of Defense as the principal staff assistants and advisors to the Secretary of Defense regarding matters related to their respective functional areas. Within these areas, the Under Secretaries exercise policy and oversight functions, and in discharging their responsibilities, the Under Secretaries may issue instructions and directive memoranda that implement policy approved by the Secretary. If confirmed, I look forward to working with the Under Secretary of Defense for Policy, in coordination with Commander, U.S. Strategic Command, on all policy issues that affect U.S. Cyber Command operations.

*Question.* The Under Secretary of Defense for Intelligence.

*Answer.* Title 10, U.S.C. and current DOD directives establish the Under Secretaries of Defense as the principal staff assistants and advisors to the Secretary of Defense regarding matters related to their respective functional areas. Within these areas, the Under Secretaries exercise policy and oversight functions and, in discharging their responsibilities the Under Secretaries may issue instructions and directive memoranda that implement policy approved by the Secretary. If confirmed, I look forward to working with the Under Secretary of Defense for Intelligence, in coordination with Commander, U.S. Strategic Command, on matters in the area of U.S. Cyber Command’s assigned responsibilities.

*Question.* The Under Secretary of Defense for Acquisition, Technology, and Logistics.

*Answer.* Title 10, U.S.C. and current DOD directives establish the Under Secretaries of Defense as the principal staff assistants and advisors to the Secretary of Defense regarding matters related to their respective functional areas. Within these areas, the Under Secretaries exercise policy and oversight functions and, in discharging their responsibilities the Under Secretaries may issue instructions and directive memoranda that implement policy approved by the Secretary. If confirmed, I look forward to working with the Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with Commander, U.S. Strategic Command, on matters in the area of U.S. Cyber Command’s assigned responsibilities.

*Question.* The Assistant Secretary of Defense for Networks and Information Integration.

*Answer.* Under the authority of DOD Directive 5144.1 and consistent with titles 10, 40, and 44, U.S.C., the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) serves as the DOD Chief Information Officer (CIO) and is the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on networks and network-centric policies and concepts; command and control (C2); communications; non-intelligence space matters; enterprise-wide integration of DOD information matters; Information Technology (IT), including National Security Systems (NSS); information resource management (IRM); spectrum management; network operations; information systems; information assurance; positioning, navigation, and timing policy, including airspace and military-air traffic control activities; sensitive information integration; contingency support and migration planning; and related matters. Pursuant to chapter 113, subchapter III of 40 U.S.C., the ASD(NII)/DOD CIO has responsibilities for integrating information and related activities and services across DOD. If confirmed, I look forward to working with the Assistant Secretary of Defense for Networks and Information Integration through the Secretary and Deputy Secretary of Defense and Commander, U.S. Strategic Command, on matters in the area of U.S. Cyber Command’s assigned responsibilities.

*Question.* The Assistant Secretary of Defense for Homeland Defense.

*Answer.* The Assistant Secretary of Defense for Homeland Defense executes responsibilities including overall supervision of the homeland defense activities of the DOD while serving under the Under Secretary of Defense for Policy. Any relationship the Commander, U.S. Cyber Command requires with the Assistant Secretary of Defense for Homeland Security would exist with and through the Under Secretary of Defense for Policy. If confirmed, I look forward to working with the Assistant Secretary of Defense for Homeland Defense in concert with Commander, U.S. Strategic Command, Commander, U.S. Northern Command, and Commander, U.S. Pacific Command on related national security issues.

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

*Answer.* The Chairman is the principal military advisor to the President, National Security Council, and Secretary of Defense. Title 10, U.S.C., section 163 allows communication between the President or the Secretary of Defense and the combatant commanders to flow through the Chairman. By custom and tradition, and as in-
structed by the UCP, I would normally communicate with the Chairman in coordination with the Commander, U.S. Strategic Command.

Question. The Secretaries of the Military Departments.

Answer. Under title 10, U.S.C., section 165, subject to the authority, direction, and control of the Secretary of Defense, and subject to the authority of the combatant commanders, the Secretaries of the Military Departments are responsible for administration and support of forces that are assigned to unified and specified commands. The authority exercised by a subunified combatant commander over Service components is quite clear but requires close coordination with each Secretary to ensure that there is no infringement upon those lawful responsibilities which a Secretary alone may discharge. If confirmed, I look forward to building a strong and productive relationship with each of the Secretaries of the Military Departments in partnership with Commander, U.S. Strategic Command.

Question. The Chiefs of Staff of the Services.

Answer. The Service Chiefs are charged to provide organized, trained, and equipped forces to be employed by combatant commanders in accomplishing their assigned missions. Additionally, these officers serve as members of the Joint Chiefs of Staff and as such have a lawful obligation to provide military advice. Individually and collectively, the Service Chiefs are a tremendous source of experience and judgment. If confirmed, I will work closely and confer regularly with the Service Chiefs.

Question. The combatant commanders and specifically the Commanders of U.S. Strategic Command and U.S. Northern Command.

Answer. U.S. Cyber Command is a subordinate unified command under U.S. Strategic Command. The Commander, U.S. Cyber Command, will have planning and supporting relationships with other combatant commanders, largely identified within the UCP, the Joint Strategic Capabilities Plan, execute orders and operation orders. In general, the Commander, U.S. Cyber Command, will be the supported commander for planning, leading, and conducting DOD defensive cyber and global network operations and, in general, is a supporting commander for offensive missions. Specific relationships with Commander, U.S. Northern Command will be delineated by the Secretary of Defense or the President in execute and/or operation orders. If confirmed, I look forward to working with the combatant commanders to broaden and enhance the level and range of these relationships.

Question. The Director of the Defense Information Systems Agency.

Answer. DISA is a DOD combat support agency that provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to join warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations. Commander, U.S. Cyber Command must maintain a close relationship with the Director, DISA to coordinate and represent requirements in this mission area, in order to accomplish U.S. Strategic Command delegated UCP missions. To this end, Lieutenant General Pollett, the current Director of DISA, has committed to providing both a DISA Field Office as well as a DISA support element unique to U.S. Cyber Command. If confirmed, I will continue to work closely with the Director of DISA on matters of shared interest and importance.

OVERSIGHT

Question. The duties of the Commander, U.S. Cyber Command will include conducting integrated intelligence collection and offensive and defensive operations in cyberspace. However, the resourcing, planning, programming and budgeting, and oversight of these three basic activities is fragmented within DOD, the executive branch as a whole, and within Congress. Multiple elements within the Office of the Secretary of Defense and the Joint Staff have responsibilities for one or more of the missions of Cyber Command. The same is true for the Secretary of Defense and the Director of National Intelligence, as well as the Armed Services and Intelligence Committees in Congress. The single point of confluence would be the Commander of Cyber Command, dual-hatted as the Director of NSA.

How do you anticipate that the Department will ensure the necessary degree of coordination and timely decisionmaking across the Department to guide the operations and resourcing of Cyber Command?

Answer. Through the Secretary of Defense’s policy initiatives for cyberspace operations and implementation guidance concerning national security directives, the Department will ensure the necessary degree of coordination and timely decision-making across the Department to guide the operations and resourcing of U.S. Cyber Command. If confirmed, I envision that the Department will retain its commitment to close coordination both internally and externally to guide the operations and resourcing of this command.
Question. What is the risk, in your view, that this fragmented policy and oversight structure will result in a lack of coherent oversight of cyberspace and U.S. Cyber Command?

Answer. I believe we have a coherent policy and oversight structure in place for cyberspace and that there is no risk that we will lack coherent oversight. If confirmed, I can assure you that my actions will be guided by the authorities vested in me by the Secretary of Defense and Commander, U.S. Strategic Command and oversight of my actions will be clearly auditable for overseers.

MAJOR CHALLENGES AND PROBLEMS

Question. In your view, what are the major challenges that will confront the Commander, U.S. Cyber Command?

Answer. I believe the major challenge that will confront the Commander, U.S. Cyber Command will be improving the defense of our military networks as they exist today. Additionally, in order to defend those networks and make good decisions in exercising operational control over them, U.S. Cyber Command will require much greater situational awareness and real-time visibility of intrusions into our networks. Finally, I believe the Commander, U.S. Cyber Command will have to identify continuously policy and authority gaps to U.S. Strategic Command and our civilian leadership as computer and communication technologies evolve.

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

Answer. Answer provided in the classified supplement.

Question. What are your priorities for the U.S. Cyber Command?

Answer. Answer provided in the classified supplement.

U.S. CYBER COMMAND MISSIONS

Question. In an overarching sense, how do you define the U.S. Cyber Command missions?

Answer. Answer provided in the classified supplement.

OFFENSIVE CYBER WARFARE CAPABILITIES

Question. The attached solicitations and program descriptions show that the military services are developing capabilities to stealthily penetrate foreign computer networks, maintain a presence on those networks, collect and extract information clandestinely, and undertake offensive actions. The National Military Strategy for Cyberspace Operations, published in 2006, also indicates that the U.S. military places considerable importance on acquiring potent offensive cyber warfare capabilities.

Does DOD possess significant capabilities to conduct military operations in cyberspace at the tactical, operational, and strategic levels?

Answer. Answer provided in the classified supplement.

Question. Is there a substantial mismatch between the ability of the United States to conduct operations in cyberspace and the level of development of policies governing such operations?

Answer. President Obama’s cybersecurity 60-day study highlighted the mismatch between our technical capabilities to conduct operations and the governing laws and policies, and our civilian leadership is working hard to resolve the mismatch. In the June 25, 2009 memorandum outlining the establishment of U.S. Cyber Command, the Secretary of Defense directed the Under Secretary of Defense for Policy to lead a review of policy and strategy to develop a comprehensive approach to DOD cyberspace operations. This review is active and ongoing.

Question. Are you concerned that you are being assigned to command an organization that may be directed to conduct activities whose legality and rules have not been worked out?

Answer. Given current operations, there are sufficient law, policy, and authorities to govern DOD cyberspace operations. If confirmed, I will operate within applicable laws, policies, and authorities. I will also identify any gaps in doctrine, policy and law that may prevent national objectives from being fully realized or executed to the Commander, U.S. Strategic Command and the Secretary of Defense.

Question. When does the administration intend to close existing policy gaps?

Answer. The administration has provided a comprehensive set of cyber security initiatives that will inform policy making (e.g., Comprehensive National Cybersecurity Initiative (CNCI) and the President’s Strategy to Secure Cyberspace). In support of the Secretary of Defense, we will continue to work to identify gaps, inform the development of meaningful and enduring national cyber policy, and be prepared to adjust rapidly to changes.
SUPPORT TO THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE

Question. Under the CNCI, NSA is providing support to the Department of Homeland Security.

What is the nature and extent of that support?

Answer. Answer provided in the classified supplement.

Question. Is this support provided as a DOD activity or as an intelligence activity through the Director of National Intelligence? If the latter, what is the Secretary of Defense’s role as the President’s executive agent for signals intelligence (SIGINT) under Executive Order 12333?

Answer. The support provided by NSA to DHS is provided as a DOD activity, in coordination with the Director of National Intelligence.

Specifically, with respect to the Foreign Intelligence support to DHS, per Executive Order 12333, as amended, NSA is an element of both the Intelligence Community, of which the Director of National Intelligence serves as the head, and DOD, whose Secretary acts, in coordination with the Director of National Intelligence, as the Executive Agent for the U.S. Government for SIGINT activities. In these capacities, NSA conducts SIGINT activities for both national and departmental requirements.

Further, with respect to Information Assurance support to DHS, for such support that is given in connection with NSSs, National Security Directive 42 provides that the Secretary of Defense shall serve as the executive agent of the Government for National Security Telecommunications and Information Systems Security. NSD 42 further designates the Director NSA as the National Manager for National Security Telecommunications and Information’s Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out those responsibilities. With respect to Information Assurance support to DHS that is provided in connection with non-NSSs, NSA is authorized by EO12333 to provide technical assistance to other U.S. Government departments and agencies for either NSSs or non-NSSs.

SUPPORT TO CIVIL AUTHORITIES

Question. DOD officials have informed the committee that U.S. Cyber Command will have a mission to support civil authorities, such as the Department of Homeland Security and law enforcement agencies, to help defend government networks and critical infrastructure networks owned and operated by the private sector.

Please describe in detail your understanding of the ways that U.S. Cyber Command is most likely to assist civil authorities.

Answer. If I am confirmed as Commander, U.S. Cyber Command, I will work closely with the Commanders of U.S. Strategic Command and U.S. Northern Command to answer any request for assistance from the Department of Homeland Security. Our assistance could include technical assistance and recommendations for immediate defensive actions, as well as technical assistance and recommendations for more systemic mitigation, such as improvements in network configurations and improvements in information assurance measures or best practices. Additionally, U.S. Cyber Command would continually assess the cyber threat to DOD’s information systems to ensure we are prepared to provide cyber support to civil authorities in the event of a cyber threat to the Nation’s critical infrastructure.

Question. U.S. Northern Command was established to serve as the focal point for DOD support to civil authorities.

Will cybersecurity support to civil authorities be provided through U.S. Northern Command, as a supported command, or otherwise? If not, why not?

Answer. Answer provided in the classified supplement.

USE OF FORCE IN CYBERSPACE

Question. Does DOD have a definition for what constitutes use of force in cyberspace, and will that definition be the same for U.S. activities in cyberspace and those of other nations?

Answer. Article 2(4) of the U.N. Charter provides that states shall refrain from the threat or use of force against the territorial integrity or political independence of any State. DOD operations are conducted consistent with international law principles in regard to what is a threat or use of force in terms of hostile intent and hostile act, as reflected in the Standing Rules of Engagement/Standing Rules for the Use of Force (SRROE/SRUF).

There is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force. Thus,
whether in the cyber or any other domain, there is always potential disagreement among nations concerning what may amount to a threat or use of force.

Remainder of answer provided in the classified supplement.

**Question.** Has DOD or the administration as a whole determined what constitutes use of force in cyberspace in relation to the War Powers Act, the exercise of the right of self-defense under the U.N. Charter, and the triggering of collective defense obligations? If not, when will these fundamental policy issues be resolved?

**Answer.** The President of the United States determines what is a threat or use of force/armed attack against the United States and authorizes DOD through the SROE to exercise our national right of self-defense recognized by the U.N. Charter. This determination involves an objective and subjective analysis that considers the facts surrounding a particular cyber attack, and is made within the bounds of U.S. and international law. If the President determines a cyber event does meet the threshold of a use of force/armed attack, he may determine that the activity is of such scope, duration, or intensity that it warrants exercising our right to self-defense and/or the initiation of hostilities as an appropriate response. It is also within the President’s authority to determine, based upon the circumstances of any event, including a cyber event, and the contemplated response, what consultations and reports to Congress are necessary consistent with the provisions of the War Powers Resolution. The U.N. Charter recognizes a State’s inherent right of individual and collective self-defense, and the United States would evaluate its collective defense obligations when another State is threatened or subject to a use of force in the cyber domain just as it would in the other warfighting domains.

**Question.** Could U.S. Cyber Command lawfully employ offensive cyber weapons against computers located abroad that have been determined to be sources of an attack on the United States or U.S. deployed forces if we do not know who is responsible for the attack (i.e., a foreign government or non-state actors)?

**Answer.** The establishment of U.S. Cyber Command, in and of itself, does not change the lawful employment of military force for self-defense. In this case, if the “attack” met the criteria approved by the President in our Standing Rules of Engagement, the military would exercise its obligation of self-defense. Operationally, it is difficult to develop an effective response when we do not know who is responsible for an “attack”; however, the circumstances may be such that at least some level of mitigating action can be taken even when we are not certain who is responsible. Regardless whether we know who is responsible, international law requires that our use of force in self-defense be proportional and discriminate. Neither proportionality nor discrimination requires that we know who is responsible before we take defensive action.

**Question.** Without confident “attribution,” under international law, would DOD, in your judgment, be allowed to “fire back” without first asking the host government to deal with the attack?

**Answer.** Answer provided in the classified supplement.

**Question.** Traditionally, espionage has not been regarded as a use of force or an act of war. Generally speaking, in cyberspace operations, experts agree that gaining access to a target for intelligence collection is tantamount to gaining the ability to attack that target. If a penetration is detected, the victim cannot determine whether the purpose of the activity is limited to espionage or also constitutes preparation for an attack.

With the foregoing in mind, are there or should there be classes of U.S. or allied targets that the U.S. Government would consider off-limits from hostile penetration because of the danger that any such breaches would present to national security?

**Answer.** Answer provided in the classified supplement.

**Question.** Would or should such targets be immune to penetration by the United States in peacetime even for intelligence collection?

**Answer.** Answer provided in the classified supplement.

**AUTHORITIES OF COMMANDER, U.S. CYBER COMMAND**

**Question.** Offensive cyber warfare weapons or operations could have devastating effects, depending on the target of the attack and the method used, which conceivably could be comparable to those caused by weapons of mass destruction.

If confirmed as Commander, U.S. Cyber Command, would you have the authority to use offensive cyber weapons against the following representative classes of targets:

- Military command and control networks;
- Military air defense networks;
- Military platforms and weapons;
- Power grids;
Banks and other financial institutions and networks;
Transportation-related networks; and
National telecommunications networks?
Answer. The categories listed are all potential targets of military attack, both kinetic and cyber, under the right circumstances. It is difficult for me to conceive of an instance where it would be appropriate to attack a bank or a financial institution, unless perhaps it was being used solely to support enemy military operations.

Offensive cyber weapons would only be authorized under specific lawful orders by the Secretary of Defense and the President and would normally come with supplemental rules of engagement.

All military operations, to include actions taken in cyberspace, must comply with international law that governs military operations. Specifically, any U.S. military operation must comport with the principles of military necessity, discrimination, and proportionality. These legal principles are addressed during the planning and operational phases of all military operations.

Question. Do you have this authority now as the Joint Functional Component Commander for Network Warfare?
Answer. Answer provided in the classified supplement.

Question. At what level of command can decisions be made to pre-deploy offensive cyber weapons against these same classes of targets? Will this change after the standup of U.S. Cyber Command?
Answer. This authority rests with the Secretary of Defense and the President. It will not change after U.S. Cyber Command is established.

Question. Operations in cyberspace occur at nearly the speed of light. Speed of response is widely considered to be necessary in some circumstances when operating in cyberspace. Is there currently or do you anticipate that there will be a requirement to pre-authorize the use of force in cyberspace below the level of the National Command Authority? If so, to what level and in what circumstances?
Answer. Answer provided in the classified supplement.

Question. Is it your understanding that, as is the case with the Commander of the subunified U.S. Forces Korea Command, the subunified Commander of Cyber Command will have freedom of action to fight the war?
Answer. The Commander of U.S. Cyber Command will have freedom of action to conduct military operations in cyberspace based upon the authorities provided by the President, the Secretary of Defense, and the Commander, U.S. Strategic Command. Because cyberspace is not generally bounded by geography, the Commander of U.S. Cyber Command will have to coordinate with U.S. agencies and combatant commanders that would be affected by actions taken in cyberspace.

Question. What is the role of the Commander, U.S. Strategic Command, in directing or approving courses of action of the Commander, U.S. Cyber Command?
Answer. Commander, U.S. Strategic Command, as the combatant commander, has the responsibility to specify U.S. Cyber Command missions and tasks and delegate appropriate authority to accomplish those tasks. In accordance with joint doctrine, authority is normally given to subordinate commanders to select the methodology for accomplishing the mission, including selection and approval of courses of action. However, this authority may be limited by directives or other orders of the superior commander. Commander, U.S. Strategic Command has indicated to the Secretary of Defense he will delegate authority for all UCP cyber tasks, with the exception of advocacy for cyberspace capabilities and integration of the Theater Security Cooperation activities with Geographic Combatant Commanders.

LAW S OF WAR

Question. Has DOD determined how the laws of armed conflict (including the principles of military necessity in choosing targets, proportionality with respect to collateral damage and unintended consequences, and distinguishing between combatants and non-combatants) apply to cyber warfare with respect to both nation-states and non-state entities (e.g., terrorists, criminals), and both when the source of an attack is known and unknown?
Answer. Per DOD guidance, all military operations must be in compliance with the laws of armed conflict—this includes cyber operations as well. The law of war principles of military necessity, proportionality and distinction will apply when conducting cyber operations.

Question. If not, when will the Department produce authoritative positions on these issues?
Answer. See answer above.
BALANCING EQUITIES

**Question.** There have been many instances in history where military and political leaders had to struggle with the choice of acting on intelligence information to save lives or forestall an enemy success but at the cost of the enemy learning that their communications, information, or capabilities had been compromised. These choices are referred to as “balancing equities” or “gain-loss” calculations. U.S. Cyber Command is to be headed by the Director of the NSA, which, like all intelligence agencies, could be naturally expected to seek to protect sensitive sources and methods.

Who will be in charge of the equities/gain-loss process for cyberspace within the military?

**Answer.** Within DOD, the equities/gain-loss process is built into the deliberate and crisis action planning process and initiated by the combatant commanders. In most cases, the gain-loss recommendation within DOD is initially made by the supported combatant commander after the risk of loss is well articulated by the Intelligence Community. If there is disagreement I, as the commander of JFCC NW, serve as the focal point for DOD offensive cyberspace operations in accordance with the deconfliction process directed in NSPD–38. If the NSPD–38 deconfliction process does not resolve the interagency disagreement, the issue goes to the Chairman, Joint Chiefs of Staff, the Secretary of Defense, the NSC Deputies, the NSC Principals, and then the President, where the gain-loss determination continues to be considered. (In counterterrorism issues, the National Counterterrorism Center is brought in before the Deputies Committee considers the issue.) If confirmed as Commander of U.S. Cyber Command, I will continue to have responsibility for this process within the Department.

**Question.** If these decisions will rest with the Commander of Cyber Command, how would you expect the process to work to ensure that the combatant commands, the Military Services, and other defense agencies have the opportunity to defend their interests and are not overruled by NSA?

**Answer.** We would use the process outlined by the Joint Staff and used by other combatant commands. Intelligence Gain-Loss is a consideration of target vetting and is coordinated with the Intelligence Community agencies and with supporting combatant commands throughout the planning process. Those agencies and commands provide comments on their equities and issues for the commander’s review and validation. The supported command then makes a determination based on their mission and expected effects. If the targeting issues cannot be resolved between the Commander, U.S. Cyber Command/Director, NSA and the Federal Bureau of Investigations Cyber Division, the issue goes to the NSC Deputies Committee, and if still unresolved, the NSC Principals Committee.

**Question.** If confirmed, how will you ensure that equities/gain-loss decisions are made for the Nation as a whole? How will the interests of the vulnerable private sector, critical infrastructure, and civil agencies be weighed in the selection of targets for intelligence collection and attack in wartime?

**Answer.** Our deconfliction process, documented in a Tri-lateral Memorandum of Agreement among DOD, DoJ and the Intelligence Community, includes appropriate representation of other agencies as directed in NSPD–38. As with targeting issues within the Department, the reclama process for issues spanning Federal agencies matriculate from the Seniors to the Deputies Committee to the Principals Committee if they remain unresolved.

DETERRENCE AND ESCALATION CONTROL

**Question.** The U.S. Government currently does not appear to have a cyber warfare deterrence strategy or doctrine. Promulgating such a doctrine requires at least some broad statements of capabilities and intentions regarding the use of offensive cyber capabilities, both to influence potential adversaries and to reassure allies. Such statements are not possible given the current degree of classification of all aspects of U.S. cyber warfare capabilities.

Do you agree that it is necessary to declassify some information about U.S. cyber warfare capabilities in order to support deterrence and engagement with allies and potential adversaries?

**Answer.** I agree and fully support the President's executive order regarding security classification. This is a complex subject, and we will continue to implement directed policies and inform policymakers of operational impacts.

**Question.** Is there a process and timetable in place to accomplish this objective?

**Answer.** I am not aware of any plan or timetable to declassify detailed information about U.S. offensive cyber capabilities. Articulating new processes and timetables would flow from direction set by the White House.
Question. Most experts believe that the attacker has a substantial advantage over the defender in cyber warfare. It is also widely believed that preemptively striking first against an adversary's networks offers an advantage if the adversary's command and control networks can be degraded, and because the attacker can take steps to protect itself from a retaliatory attack. These considerations suggest that cyber warfare is currently “unstable” from the perspective of classic deterrence theory and escalation control.

Do you, or to your knowledge, experts in the Department, have a different view of these dynamics?

Answer. I’d certainly agree that cyber warfare has unique and important differences from classic deterrence theory and escalation control. Experts, both inside and outside government, as well as within DOD and Intelligence Communities, have widely differing views of these dynamics, as should be expected. A consensus has yet to emerge, either on how to characterize the strategic “instability” or on what to do about it.

U.S. MILITARY STRATEGY IN CYBERSPAC

Question. The National Military Strategy for Cyberspace Operations (NMS–CO), December 2006, states that “The United States must have cyberspace superiority to ensure our freedom of action and deny the same to our adversaries through the integration of network defense, exploitation, and attack.... The NMS–CO is the comprehensive military strategy for the U.S. Armed Forces to ensure U.S. superiority in cyberspace.”

Is this strategy statement consistent with current policy? If not, is there a plan to issue a new or revised NMS–CO?

Answer. Answer provided in the classified supplement.

Question. Is this strategy realistic in light of the vulnerability of U.S. Government and private networks to attack?

Answer. The military strategic goal of cyberspace superiority is realistic, but not without difficulty in achieving its objectives in the current national security environment. The 42 tasks in the NMS–CO Implementation Plan continue to inform how DOD will move towards achieving cyberspace superiority. Many of these tasks are defensive, directed at addressing the vulnerabilities of the DOD networks, and take into consideration the fact that the internet is a completely connected environment where both DOD and private networks reside.

Question. In an interview on “60 Minutes,” former Director of National Intelligence Michael McConnell said that “If I were an attacker and I wanted to do strategic damage to the United States... I would sack electric power on the U.S. east coast, maybe the west coast, and attempt to cause a cascading effect. All of those things are in the art of the possible from a sophisticated attacker.” He was then asked whether he believes that adversaries have the ability to bring down the power grid, and he replied “I do.” Crippling the U.S. power grid would not only cause catastrophic economic problems; presumably it would lead to significant loss of life, especially if the outage was prolonged. Likewise, it could cripple DOD’s ability to generate and sustain forces.

In light of our current vulnerability to cyber attack, what is the risk in your view that DOD and U.S. Cyber Command could be deterred from undertaking coercive action against countries such as Iran or North Korea because of the possibility that they could successfully launch devastating attacks on critical U.S. infrastructure?

Answer. Answer provided in the classified supplement.

Question. Is this level of vulnerability consistent with the NMS–CO assertion that the United States ensures “superiority” in cyberspace?

Answer. Yes, it is consistent that the United States seeks to ensure superiority in cyberspace: Even with the clear understanding that we could experience damage to our infrastructure, we must be prepared to “fight through” in the worst case scenario. Based on vulnerability, step one is to ensure that we can defend our networks. In fact, the use of the term superiority, versus dominance or supremacy, reflects the limits of our capabilities throughout the domain. Having recognized the gap between the end states of the NMS–CO and current capabilities, the Department developed an implementation plan to close these gaps. The current state of our networks presents a strategic vulnerability for the Department and the Nation. If confirmed, I will focus U.S. Cyber Command on securing the Department’s networks and, as requested, assisting other Federal agencies to secure the networks for which they are responsible.

Question. The NMS–CO states that “U.S. law and national policy assign DOD three main roles: defense of the Nation, national incident response, and critical infrastructure protection.... Although partner departments and agencies have respon
sibilities to secure portions of cyberspace, only DOD conducts military operations to defend cyberspace, the critical infrastructure, the homeland, or other vital U.S. interests. If defense of a vital interest is implicated, DOD’s national defense mission takes primacy even if that would conflict with, or subsume, the other support missions.

Are these statements consistent with DOD’s statements that U.S. Cyber Command will not have the mission to defend the “.gov” and “.com” networks?

Answer. Yes, they are consistent. Although U.S. Cyber Command’s mission will not include defense of the .gov and .com domains, given the integration of cyberspace into the operation of much of our critical infrastructure and the conduct of commerce and governance, it is the obligation of the Department to be prepared to provide military options to the President and Secretary of Defense if our national security is threatened. Any defensive action in support of a domain other than .mil would require a proper request for assistance or a directive from the President.

Question. Has “critical infrastructure” been formally defined or otherwise identified for the purposes of cybersecurity?

Answer. Yes, specifically “critical infrastructure” has been formally defined in HSPD–7 as those systems or assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Question. Do these statements reflect current policy?

Answer. Yes, they reflect current policy.

Question. Do these statements mean that DOD’s mission to defend the Nation “takes primacy” over the Department of Homeland Security’s role in some situations?

Answer. Yes, when war or any attack or other national security crisis arises whereby the use of force is contemplated, DOD would take the lead in defending the Nation. However, a Presidential order calling on DOD to take the lead role in responding to a cyber attack on the United States would be required before DOD assumes this lead role. I believe that DOD and DHS are completely in synch on this point.

Question. The NMS–CO states that “under the authorities of the Secretary of Defense, DOD will use network exploitation to gather intelligence and shape the cyber-space environment as necessary to provide integrated offensive and defensive options.” This statement appears to mean that DOD will attempt to gain access to foreign networks to create the ability to conduct offensive operations.

Under what conditions would DOD prepare foreign networks for offensive operations when access is acquired for intelligence gathering?

Answer. DOD conducts extensive planning for a wide range of contingencies including planning for cyberspace operations. Effective planning for offensive cyber operations requires extensive knowledge and understanding of foreign networks and is accomplished by foreign intelligence collection. Any preparation of foreign networks outside that is beyond the realm of intelligence gathering can only be conducted by lawful order (EXORD) from Secretary of Defense and the President.

Question. Are such actions authorized and reported to Congress under title 10 or title 50?

Answer. Preparation of foreign networks for offensive operations is authorized only when part of a Secretary of Defense-approved military operation under title 10 of the U.S.C.; such military operations are subject to congressional armed services committee oversight. Foreign intelligence collection activities are subjected to congressional intelligence oversight.

Question. Does the Secretary of Defense have the unilateral authority to direct intelligence-gathering operations in cyberspace?

Answer. The Secretary of Defense, as authorized by law and executive order, can direct intelligence activities in cyberspace for those intelligence activities, such as SIGINT, under his operational control.

Question. If the Secretary of Defense is the President’s executive agent for SIGINT, what is the role of the Director of National Intelligence in directing SIGINT collection in cyberspace?

Answer. The DNI provides the National Intelligence Strategy and the National Intelligence Priority Framework, among others, to the entire Intelligence Community. The DNI also plays a role with respect to resource allocation via the National Intelligence Program.

Question. Under the Secretary’s role as the executive agent for SIGINT, what was the Secretary’s responsibility for the policy decisions regarding the NSA’s Terrorist Surveillance Program, and the assistance that NSA is providing to the Department
of Homeland Security through the Einstein 3 intrusion detection and prevention program?

Answer. Answer provided in the classified supplement.

*Question.* The NMS–CO states that "Adversaries are deterred from establishing or employing offensive capabilities against U.S. interests in cyberspace. DOD will deter malicious adversary use of cyberspace, while promoting freedom of action and trust and confidence in U.S. cyberspace operations. Through deterrence, DOD seeks to influence the adversary’s decisionmaking processes by imposing political, economic, or military costs; denying the benefits of their actions; and inducing adversary restraint based on demonstrated U.S. capabilities."

In your opinion, is it the case that "adversaries are deterred" from acting against U.S. interests in cyberspace?

Answer. Answer provided in the classified supplement.

*Question.* Does the United States have a deterrence doctrine and a deterrence strategy for cyber warfare?

Answer. Answer provided in the classified supplement.

*Question.* Has the United States ever “demonstrated capabilities” in cyberspace in a way that would lead to deterrence of potential adversaries?

Answer. Not in any significant way. We have conducted exercises and war games, and responded to threats, intrusions, and even attacks against us in cyberspace. Law Enforcement and the Counter-Intelligence community have responded to intrusions and insider threats. Even industry and academia have attempted to “police” the Internet. How all of these have deterred criminal actions, terrorists, hostile intelligence entities, and even nation states cannot be systematically measured.

**IMPLICATIONS OF U.S. DEPENDENCE ON CYBER NETWORKS**

*Question.* Many experts assert that the United States is the most vulnerable country in the world to cyber attack because we are the most networked nation and the one that has most fully-exploited computer networks for business, government, and military functions. This judgment implies that the United States has the most to lose in a serious cyber conflict.

How could DOD best compensate for U.S. dependence on vulnerable cyber networks in developing effective deterrent strategies?

Answer. Answer provided in the classified supplement.

*Question.* Given U.S. vulnerabilities, is it in our interest to engage in certain kinds of offensive cyber warfare, and possibly set precedents by example that other nations might follow?

Answer. Answer provided in the classified supplement.

**COVERT ACTION VERSUS TRADITIONAL MILITARY OPERATIONS**

*Question.* What is your understanding of whether clandestine offensive actions in cyberspace conducted by DOD in connection with an ongoing military conflict where the hand of the U.S. Government is intended to be concealed “covert action” under the law, or are they considered traditional military operations?

Answer. Covert action, as defined by law, includes "an activity or activities of the U.S. Government to influence political, economic, or military conditions abroad, where it is intended that the role of the U.S. Government will not be apparent or acknowledged publicly." The law goes on specifically to except “traditional … military activities” from being considered covert actions. (50 U.S.C. 413b(e)(2000)) Traditional military activities are often clandestine in order to guarantee mission success and protect tactics, techniques, and procedures—this is no different in cyberspace. DOD believes the traditional military activities exception applies to the emerging field of cyberspace operations.

*Question.* Does it matter whether such actions are conducted within or outside of a theater of ongoing, traditional armed conflict?

Answer. This is a matter of ongoing debate. Proposed actions to deliver effects to combatant commanders at the tactical and operational level should be pursued as traditional military operations, under existing authorizations, if possible. Any actions that we take must be approved by the Secretary of Defense and the President through a lawful order.

**REQUIREMENT FOR TRANSIT RIGHTS**

*Question.* Under international law, nations enjoy sovereign rights over the territorial extent of their countries and the airspace above it, although not in space. Transiting that sovereign territory and airspace for military purposes requires permission.
In a situation where a government intends to deliver a cyber weapon or capability to a country not adjacent to its territory, through terrestrial telecommunications networks, what is the legality of doing so without the permission of the governments of the Nations through which the weapon must pass?

Answer. Answer provided in the classified supplement.

THE CHALLENGE OF ATTRIBUTION

Question. An essential feature of military, intelligence, and criminal or malicious activities in cyberspace is the ease with which the origin and the identity of those responsible for an attack can be concealed. This “attribution” problem is severe. If it is impossible to say with certainty who committed an attack, no one can be held responsible, making deterrence and retaliation alike problematic. The attribution capabilities that do exist appear to be time- and resource-intensive, which can make appropriate, timely responses difficult or even impossible. How can deterrence be established in the absence of reliable attribution?

Answer. I agree that attribution can be very difficult. We must approach this problem in two ways. First and foremost, the most effective way to deter adversaries is to increase the security of our own networks. This will act as a deterrent to those adversaries who target the United States simply because we are an easy mark. This is a national problem and better security solutions must be encouraged for all U.S. public and private networks.

Concurrently, we must partner closely with the Intelligence Community to improve our ability to determine attribution. We must also establish partnerships with nation-states that share common goals for lawful behavior in cyberspace. Such agreements would establish expectations of normative behavior for cyber activities and thresholds for bad behaviors that would not be allowed to continue. Such expectations will require standards of evidence that are mutually acceptable and include highly automated procedures that allow attacks to be alerted on and halted quickly.

Criminal law models depend on deterrence, as well. Legal scholars have argued that crimes that often go unsolved (vandalism, for example) should be punished more harshly to ensure an effective example is offered in the few cases when it’s available. Under this model, the United States should take swift and effective action in every case in which it can attribute an offensive action to a particular adversary.

Attribution has been a problem since the beginning of the terrorism era. For example, in 1983 when the Marine barracks in Beirut was bombed, the United States would likely have taken strong action against the perpetrator—but the perpetrator was dead and the planners were unknown. This problem continues today in kinetic operations as well as in cyber.

The bottom line is, the only way to deter cyber attack is to work to catch perpetrators and take strong and public action when we do.

Question. What authorities are required, or what procedures must be invoked, to track back through layers of an attack involving computers located in the United States and owned by U.S. persons?

Answer. Investigations of cyber attacks originating or appearing to originate from the United States are typically law enforcement investigations and a law enforcement warrant is used to attempt to track back through layers involving computers located in the United States or owned by U.S. persons. If there is reason to believe that the attack is being conducted by a foreign power or agent of a foreign power, though appearing to originate from the United States, the investigation can be a counterintelligence investigation and the Foreign Intelligence Surveillance Act order would be used to track back through layers involving computers located in the United States or owned by a U.S. person.

Question. What are the legalities, both in domestic and international law, involved in “shooting back” immediately at the sources of a large-scale attack, with and without a determination that the sources are commandeered computers?

Answer. A commander’s right to general self-defense is clearly established in both U.S. and international law. Although this right has not been specifically established by legal precedent to apply to attacks in cyberspace, it is reasonable to assume that returning fire in cyberspace, as long as it complied with law of war principles (e.g., proportionality), would be lawful.

Remainder of answer provided in the classified supplement.

Question. The law regarding self-defense in the case of an attack has never required a determination of identity before action can be taken. For example, if someone is shooting at you, it isn’t necessary to establish what his name is before shooting back. If someone in a car is trying to run down a police officer, the officer is not required to determine whether the car is stolen before shooting out the tires in
self-defense. Similarly, the fact that computers may be commandeered is irrelevant to the exercise of self-defense.

The United States has always hoped that the Internet would play a “subversive” role in countries with authoritarian governments. If the U.S. Government takes vigorous diplomatic action, as some experts recommend, to establish the norm that governments are responsible for what happens in cyberspace within their sovereign domains as a way to deal with the attribution problem, is there a danger we could be providing a strong justification for governments abroad to intensify surveillance and increase government controls on the Internet?

Answer. Governments that have a tendency to curtail the freedoms of their citizens will likely take such actions regardless of U.S. policies regarding cyberspace. However, the United States has the opportunity to model for other nations the process by which a nation-state can allow freedom of expression, and even advanced concepts such as Net Neutrality, and still insist on cyberspace behaviors that meet the norms of international expectations in that they could not be construed as constituting an attack in cyberspace. We can do this without increased individual surveillance.

Question. Is it accurate that a large proportion of world-wide unauthorized cyber intrusions and malicious cyber activity originates or appears to originate within the United States?

Answer. Answer provided in the classified supplement.

Question. Is it reasonable to hold other governments responsible for all such activity originating in their countries if the U.S. Government cannot or will not stop it here?

Answer. Every government is responsible for actions originating in its own country. We make every effort to address activity originating in the United States, and we expect other countries will do the same.

TITLE 10 VERSUS TITLE 50 REPORTING AND OVERSIGHT

Question. As the attached solicitations and program descriptions indicate, and the National Military Strategy for Cyberspace Operations implies, gaining access to a cyberspace target for the purpose of collecting intelligence also provides the basis for attacking that target, and vice versa. Intelligence collection in cyberspace is authorized and overseen under title 50 procedures, whereas operational preparation of the environment for military action is authorized and overseen under title 10 procedures.

Has the administration determined how it is going to authorize these actions and report them to Congress?

Answer. Intelligence collection in cyberspace is conducted as part of a foreign intelligence mission and is subject to congressional intelligence oversight; e.g., the SIGINT Computer Network Exploitation mission is conducted in accordance with SIGINT procedures and is reported to the intelligence oversight committees. Military actions in cyberspace done to prepare the environment for possible cyber attack are authorized through Secretary of Defense Execute Orders and reportable to the Armed Services Committees.

The attached solicitations and program descriptions indicate that non-intelligence elements of DOD are developing capabilities to penetrate foreign networks clandestinely, remain there undetected, and exfiltrate data secretly.

Question. Are non-intelligence elements of DOD authorized to collect intelligence in cyberspace through the clandestine penetration of networks?

Answer. Non-intelligence elements of the DOD are not authorized to collect intelligence or conduct preparation of the environment without an appropriate execute order.

SYSTEMS ACQUISITION

Question. Combatant commands by design play a restricted role in the acquisition process. However, the Commander, U.S. Cyber Command, is to be dual-hatted as the Director of NSA, which is a large enterprise with substantial resources for developing, procuring, and supporting new equipment, systems, and capabilities. In addition, the Commander will exercise operational control of DISA networks, which also acquires systems and capabilities.

Answer. Commander, U.S. Cyber Command will not exercise command or operational control over the DISA communications networks. DISA will continue to be responsible for acquiring, engineering and provisioning enterprise infrastructure to assure the availability of military information networks. As a Combat Support Agency, DISA will maintain a close working relationship with U.S. Cyber Com-
mand, providing expertise on the networks, communications and computing infrastructure operated by DISA through both a DISA Field Office and a DISA Support Element.

**Question.** Is there a precedent for a combatant commander to exercise this degree of direct control over acquisition organizations, aside from Special Operations Command, which Congress expressly provided with acquisition authority?

**Answer.** Commander, U.S. Cyber Command, would depend upon the Military Departments and Agencies to deliver on U.S. Cyber Command-documented requirements for capabilities. Each of the military departments and agencies has oversight to ensure that this is done properly. This is consistent with other combatant and subunified commands, with the exception of U.S. Special Operations Command.

**Question.** What measures is the Department taking to guarantee that Commanders of U.S. Cyber Command do not circumvent the requirements process and the established acquisition process by directing subordinates at NSA or DISA to directly address needs perceived by Cyber Command?

**Answer.** U.S. Cyber Command will be a separate organization with a separate and distinct acquisition authorities/process and staff from the NSA and DISA. The separate oversight, accountability chains, and the ability to audit actions taken by the two distinct organizations of NSA and the future U.S. Cyber Command exist to ensure that the Commander, U.S. Cyber Command follows the Cyber Command requirements process and that the Director of NSA follows the established NSA acquisition process. Specifically, NSA and U.S. Cyber Command will have separate staffs with distinct authorities and oversight. U.S. Cyber Command will operate under the same authorities and oversight as other Combatant Commands and Subunified Commands.

NSA must operate under the authority and oversight of DOD and Director, National Intelligence. Operating under distinct authorities is not a new condition for the Director of NSA. I, like all the DIRNSAs before me, am used to working under distinct authorities (title 10 and title 50) and oversight (DOD and DNI), because of NSA's two separate missions in Foreign Intelligence and Information Assurance.

Furthermore, as Director of NSA, I have delegated acquisition authority to the Senior Acquisition Executive (SAE), who is not assigned to or aligned with U.S. Cyber Command. The SAE position was established in response to recommendations by Congress in 2000. Additionally, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&T)) and the Office of the Director of National Intelligence (ODNI) both have Milestone Decision Authority (MDA) for some NSA Major System Acquisitions (MSA). While ODNI and USD(AT&T) have delegated the NSA SAE Milestone Decision Authority for certain major acquisition programs through the annual delegation process, they retain joint acquisition oversight over all MSAs. Both organizations conduct quarterly reviews of all MSA/Acquisition Category I and Special Interest Programs, and USD(AT&T) conducts a tri-annual review of NSA's contracting process in accordance with the Defense Financial Acquisition Regulation Supplement.

The Director of DISA reports to ASD(NII) and will not be a subordinate of Commander, U.S. Cyber Command. Additionally, Commander, U.S. Cyber Command will have no subordinates in DISA.

**EXTENDED DETERRENCE IN CYBERSPACE**

**Question.** With respect to close allies who depend upon the United States for their security, will DOD provide a defense capability against attacks on their critical military, government, and economic infrastructure?

**Answer.** Answer provided in the classified supplement.

**Question.** Is DOD considering an “extended deterrence” model similar to that which we have offered through the U.S. “nuclear umbrella”?

**Answer.** I am not aware of any efforts to develop an extended deterrence model for cyber.

**Question.** The financial sector in the United States is tightly integrated with and dependent upon the global financial network, such that a massive attack on financial networks abroad would probably inflict great harm on the United States. To what extent does DOD consider that the defense of some U.S. critical infrastructures must encompass network extensions abroad?

**Answer.** Answer provided in the classified supplement.

**AUTHORITIES AND PROCEDURES FOR INVESTIGATING “.MIL” INTRUSIONS**

**Question.** One of the difficult issues confronting the Einstein 3 intrusion detection and prevention program is what to do when packets are detected that contain malicious code. Attackers usually act indirectly against their targets, routing attacks
through a series of innocent intermediaries to hide their identities and locations. A malicious penetration or attack on a "gov" computer or network may be launched from a specific computer but without the knowledge of the legitimate owner of that computer. However, government personnel discovering such an attack have no way of knowing, without further investigation, which computer owners in a chain may be complicit. The Federal Government has not announced how it will specifically respond in terms of investigating actual or apparent attacks, retaining and analyzing associated data, when a warrant is required, and so forth, for the defense of the civil "gov" networks. However, DOD has already fielded intrusion detection and prevention capabilities developed by NSA at the gateways to the "mil" networks.

Does this mean that the Department has developed and received approval for protocols and procedures for investigating U.S. persons whose computers may be implicated in attacks on "mil" targets?

Answer. Answer provided in the classified supplement.

EXPLAINING CYBERSECURITY PLANS TO THE AMERICAN PEOPLE

Question. The majority of the funding for the multi-billion dollar CNCI is contained in the classified National Intelligence Program budget, which is reviewed and approved by the congressional intelligence committees. Almost all important aspects of the CNCI remain highly classified, including the implementation plan for the Einstein 3 intrusion detection and prevention system. It is widely perceived that the Department of Homeland Security is actually likely to simply extend the cyber security system that the NSA developed for DOD into the civilian and even the private sector for defense of critical infrastructure. DOD is creating a subunified Cyber Command with the Director of NSA as its Commander.

In your view, are we risking creating the perception, at home and abroad, that the U.S. Government’s dominant interests and objectives in cyberspace are intelligence- and military-related, and if so, is this a perception that we want to exist?

Answer. No, I don’t believe we are risking creating this perception as long as we communicate clearly to the American people—and the world—regarding our interests and objectives.

Question. Based on your experience, are the American people likely to accept deployment of classified methods of monitoring electronic communications to defend the government and critical infrastructure without explaining basic aspects of how this monitoring will be conducted and how it may affect them?

Answer. I believe the government and the American people expect both NSA and U.S. Cyber Command to support the cyber defense of our Nation. Our support does not in any way suggest that we would be monitoring Americans.

I don’t believe we should ask the public to accept blindly some unclear “classified” method. We need to be transparent and communicate to the American people about our objectives to address the national security threat to our Nation—the nature of the threat, our overall approach, and the roles and responsibilities of each department and agency involved—including NSA and DOD. I am personally committed to this transparency, and I know that DOD, the Intelligence Community, and rest of the administration are as well. What needs to remain classified, and I believe that the American people will accept this as reasonable, are the specific foreign threats that we are looking for and how we identify them, and what actions we take when they are identified. For these areas, the American people have you, their elected representatives, to provide the appropriate oversight on their behalf.

Remainder of answer provided in the classified supplement.

Question. What are your views as to the necessity and desirability of maintaining the current level of classification of the CNCI?

Answer. In recent months, we have seen an increasing amount of information being shared by the administration and the departments and agencies on the CNCI and cybersecurity in general, which I believe is consistent with our commitment to transparency. I expect that trend to continue, and personally believe and support this transparency as a foundational element of the dialogue that we need to have with the American people on cybersecurity.

MILITARY SERVICE ROLES IN CYBER COMMAND

Question. Each of the military services is planning to create new organizations and structures, or expand existing ones, to support the new U.S. Cyber Command. However, cyberspace is a virtual realm, considerably removed from the physical world.

Has the Department undertaken any analyses of alternative means of providing forces and capabilities to the new Command?
Answer. In accordance with the Secretary of Defense memorandum directing the establishment of U.S. Cyber Command, each of the Services conducted a thorough mission analysis on how best to provide capabilities to U.S. Cyber Command, selected a course of action for the near term, and briefed that selection to the Deputy Secretary.

Further, U.S. Strategic Command, in coordination with the Services and other combatant commanders, completed a study last year that gives us an initial vector for required force size and composition for a portion of the force. To that end, the Joint Requirements and Oversight Committee approved that recommendation and directed a more in-depth study. The study, the Cyber Analysis Campaign, is underway and should give us a force sizing construct by the end of the summer.

Question. Can it be said that there is a logical basis for ground, sea, and air components in cyberspace—apart from the fact that each of the Services operate networks that must be defended?

Answer. There is a logical basis for the department to organize both efficiently and consistently to achieve its assigned mission. In much the same manner that—from a mission standpoint—Special Operations or logistics crosses all warfighting dimensions, so does cyberspace. There may come a time when this would merit further consideration based upon lessons to be learned. Currently, the Military Department to organize, man, train, and equip to generate and sustain mission capacity on behalf of the Nation. Like other operational commands, it will be U.S. Cyber Command’s business to take this cyber capacity—built to a common standard—and turn that into joint, combined cyber capability to achieve the supported commander’s assigned mission as authorized by the Secretary of Defense.

Question. Is it optimal that each service have a separate organization for supporting U.S. Cyber Command, especially in the areas of intelligence and offensive cyber warfare?

Answer. Yes, I believe so. If cyberspace was homogenous and the entirety of the work force did the same job, one could make the argument that the Department doesn’t need each Service to have its own cyber component. But that would be a vast oversimplification of the complexity of the domain. At the operational and tactical levels of war, the Service components will be responsible for significant cyber operations. They will depend upon the networks for command and control of their forces and must be able to defend those networks. Over time the Services will also bring resources to bear in the intelligence and offensive cyber realm that will support their component missions at the operational and tactical levels of war, with deconfliction by U.S. Cyber Command. Each Service brings a unique perspective and some specialized capability to the fight that would be neither efficient nor effective to flatten into a singular whole. In cyberspace, as in all the domains, each Service brings capability to be employed in the combined arms philosophy that makes the whole greater than the sum of the parts.

COMMAND OF NATIONAL DEFENSE IN CYBERSPACE

Question. A cornerstone of military doctrine is the importance of unity of command, particularly in time-sensitive scenarios such as those that are likely to arise in cyberspace. In the Federal Government, the Department of Homeland Security is in charge of defending the country against cyber attacks, but authorities and responsibilities are fragmented and spread across the Intelligence Community, DOD, the Department of Homeland Security, the Justice Department, the Treasury Department, and the Department of Energy. Also, each department and independent agency is responsible for operating and equipping its own networks.

In your opinion, is there adequate unity of command and authorities for the Nation’s response to serious cyber attacks?

Answer. Unity of command within DOD is being improved with the establishment of U.S. Cyber Command; however, unity of effort, vice command, is equally important and achievable since effective cyber security requires a whole-of-government approach.

As securing and defending our national cyber interests is an evolving work in progress, coordination, cooperation, and information sharing across the Federal Government is paramount. A rigorous partnership with DHS—as they look to secure and protect the .gov domain and critical infrastructure—is particularly crucial. DOD continually reviews its existing authorities and directives to determine what, if any, changes need to be requested to support ongoing or contingency plans. Our unique challenge in this domain is to develop a thorough understanding of the domain, posture to be prepared to recognize as rapidly as possible those vulnerabilities or threat unknowns and set effective “post-crisis” frameworks and conditions for decisionmakers, policymakers, and legislators pre-crisis.
Question. If not, what is the process and schedule for defining and establishing an effective construct?

Answer. Ultimately, the best processes and policies are those that enable our national decisionmakers and operating forces to achieve the best desired outcome. DOD continues to support and help protect our national cyber interests as authorized and directed.

DESIGNING THE INTERNET FOR BETTER SECURITY

Question. Cyber security experts emphasize that the Internet was not designed for security. How could the Internet be designed differently to provide much greater inherent security?

Answer. The design of the Internet is—and will continue to evolve—based on technological advancements. These new technologies will enhance mobility and, if properly implemented, security. It is in the best interest of both government and industry to consider security more prominently in this evolving future internet architecture. If confirmed, I look forward to working with this committee, as well as industry leaders, academia, the Services, and DOD agencies on these important concerns.

Question. Is it practical to consider adopting those modifications?

Answer. Answer provided in the classified supplement.

Question. What would the impact be on privacy, both pro and con?

Answer. Answer provided in the classified supplement.

CONGRESSIONAL OVERSIGHT

Question. In order to exercise its legislative and oversight responsibilities, it is important that this committee and other appropriate committees of Congress are able to receive testimony, briefings, and other communications of information. Do you agree, if confirmed for this high position, to appear before this committee and other appropriate committees of Congress?

Answer. Yes.

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

Answer. Yes.

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

Answer. Yes.

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

Answer. Yes.

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

Answer. Yes.

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR CARL LEVIN

INTELLIGENCE COLLECTION GOALS VERSUS MILITARY WARFIGHTING GOALS

1. Senator Levin. Lieutenant General Alexander, there was a recent Washington Post report of a supposed offensive cyber operation to take down an internet site that, according to the report, was providing valuable information to the Intelligence Community. Whether this article is accurate or not, the article highlights the concern about arbitrating between the potentially competing priorities of protecting useful intelligence sources, versus taking offensive or defensive action to achieve military objectives. What do you believe is the appropriate mechanism for arbitrating between protecting a potentially valuable source of intelligence and conducting cyber operations in support of some military objective? General Alexander. [Deleted.]
2. Senator Levin. Lieutenant General Alexander, do you agree that it is appropriate that this committee be informed of all significant U.S. offensive cyber operations in a timely manner?

General Alexander. Yes, I agree that in almost all circumstances the Armed Services Committees should be informed in a timely manner of significant offensive cyber operations conducted by Cyber Command (CYBERCOM).

OVERSIGHT FOR OFFENSIVE CYBER OPERATIONS

3. Senator Levin. Lieutenant General Alexander, one of the committee's major concerns is that an action to penetrate a network in order to collect intelligence in many situations is deemed by experts to be virtually identical to the steps one would take to prepare that target for offensive operations. In the advance policy questions, we asked you under what authorities these activities would be conducted, reported, and overseen by Congress.

You replied that that preparation of a target network for offensive operations is ordered only by the Secretary of Defense in an Execute Order and is reported to the House and Senate Armed Services Committees, while penetration for intelligence collection is approved under intelligence authorities and reported to the intelligence committees.

Unfortunately, the reality is not that clear. There is no neat and clear distinction between these two activities in cyberspace. In fact, a distinction does not really exist, which is why we posed the question in the first place to ensure that you, the Department of Defense (DOD), and the administration address this problem.

Unfortunately, we also learned, after asking a specific question following the appearance of a Washington Post article reporting on an apparent offensive cyber operation, that DOD has undertaken a number of offensive cyber operations in the last several years, none of which was reported to the Armed Services Committees, notwithstanding your answer to the question. Have the Armed Services Committees been informed of all U.S. offensive cyber operations?

General Alexander. [Deleted.]

4. Senator Levin. Lieutenant General Alexander, do you agree that it is appropriate that the Armed Services Committees be informed of all U.S. offensive cyber operations?

General Alexander. Yes, I agree that in almost all circumstances the Armed Services Committees should be informed in a timely manner of significant offensive cyber operations conducted by CYBERCOM.

ACQUISITION CONFLICTS OF INTEREST

5. Senator Levin. Lieutenant General Alexander, if confirmed, you would lead the development of requirements for CYBERCOM. At the same time, you would remain as the Director of the National Security Agency (NSA), which has a sizeable acquisition budget. Why should we have confidence that you will be able to arbitrate effectively between your requirements definition role at CYBERCOM and your acquisition provider role at NSA?

General Alexander. While the Commander, CYBERCOM, and the Director, NSA, roles are slated to be dual-hatted under the same individual, each organization will have separate and distinct staffs.

Acquisition Authority for the NSA has been delegated by the Director, NSA, to the NSA Senior Acquisition Executive (SAE), who is not assigned to nor aligned with CYBERCOM. The SAE position was established in response to requests/recommendations by Congress in 2000. Additionally, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and the Office of the Director for National Intelligence both have Milestone Decision Authority (MDA) for NSA Major Systems Acquisitions. These two safeguards will ensure that acquisition processes and external oversight are properly executed.

CYBERCOM, as a subunified command of STRATCOM, will not have acquisition or procurement authority and will work through its Executive Agent, the U.S. Air Force, to satisfy its requirements.

6. Senator Levin. Lieutenant General Alexander, what thoughts do you have for how we can build the appropriate firewalls between your multiple roles, and how we can develop an acquisition process for cyberspace that provides the high degree of agility required to keep pace with the technology while preserving acquisition discipline and oversight?
General ALEXANDER. [Deleted.]

DECISION ON USE OF FORCE

7. Senator LEVIN. Lieutenant General Alexander, in our advance policy questions, we asked you if you would have authority to fight the war as does U.S. Forces Korea, the only other subunified command. You said that you would have the authorities provided by the President, the Secretary of Defense, and the Commander of the U.S. Strategic Command (STRATCOM).

In answer to another question, you said that under joint doctrine “authority is normally given to subordinate commanders to select the methodology for accomplishing the mission,” implying that you would have the freedom to decide how to accomplish mission orders. You went on to say that the Commander of STRATCOM has indicated already that he would delegate to CYBERCOM “authority for all UCP [Unified Command Plan] cyber tasks.” If you were to view these answers collectively, CYBERCOM could have the discretion to use offensive weapons to achieve any or all assigned cyber tasks.

If you are confirmed, will authority to employ such weapons be delegated to you? If so, under what circumstances would you have authority to act without having further direction from the President, the Secretary of Defense, or the Commander of STRATCOM?

General ALEXANDER. [Deleted.]

AUTHORITIES OF THE DIRECTOR OF NATIONAL INTELLIGENCE

8. Senator LEVIN. Lieutenant General Alexander, in the advance policy questions, you were asked to characterize the role of the Director of National Intelligence (DNI) in signals intelligence (SIGINT) in cyberspace in light of the emphasis DOD is placing on the role of the Secretary of Defense as the President’s Executive Agent for Signals Intelligence under Executive Order 12333. You said that the DNI’s role is to issue the National Intelligence Priorities Framework and to oversee resource allocation.

Your answer appears to overlook the fact that the Intelligence Reform and Terrorism Prevention Act of 2004 explicitly provides the DNI with the operational authority to task all national intelligence collection and analysis. That includes SIGINT.

Could you elaborate on the respective roles and authorities of the Secretary of Defense and the DNI with this in mind?

General ALEXANDER. [Deleted.]

Both the DNI and the Secretary of Defense have roles and responsibilities for the direction and management of the Nation’s SIGINT activities. These roles and responsibilities were provided for in the “Intelligence Reform and Terrorism Prevention Act of 2004” (IRTPA), and implemented through amendment of Executive Order 12333 (EO12333), “United States Intelligence Activities.” Section 1018 of IRTPA said the President shall issue guidelines to ensure the effective implementation and execution within the executive branch of the authorities provided to the DNI without abrogating the statutory responsibilities of the Secretary of Defense. The President did so with EO12333, as amended by EO13470. For example, the DNI shall determine requirements and priorities for, and manage and direct the tasking, collection, analysis, production, and dissemination of, national intelligence by elements of the Intelligence Community. At the same time, the Secretary of Defense is the U.S. Government’s executive agent for SIGINT but, as provided for in section 1.10(e) of EO12333, exercises his executive agent responsibilities “in coordination with” the DNI. As a result, as the Director of NSA, I take direction from both the Secretary of Defense and the DNI to ensure that I am collecting and producing SIGINT that is responsive to national and DOD requirements (to include support to military operations).

9. Senator LEVIN. Lieutenant General Alexander, does the Secretary of Defense have the authority to direct SIGINT collection and analysis unilaterally, or only at the direction or approval of the DNI?

General ALEXANDER. [Deleted.]

ROLE OF COMMERCIAL INDUSTRY IN CYBER SECURITY

10. Senator LEVIN. Lieutenant General Alexander, it is widely believed and reported that the NSA has advised the last administration and the current one that
only the NSA has the technology and know-how to provide effective defenses for the Government and the companies that own and operate critical infrastructure—like banking, transportation, power distribution, and telecommunications. However, the committee understands that the major telecommunications companies, as well as leading information technology companies, believe that their industries possess major capabilities that in some respects exceed those of the Government.

For example, the so-called tier 1 communications providers who own and operate most of the world’s telecommunications networks on which the Internet operates have unparalleled insight into what is happening in cyberspace on a global scale, and have tools to detect and stop threats as they are materializing. Do you agree that the commercial sector has untapped potential to help solve our cyber security problems?

General ALEXANDER. [Deleted.]

11. Senator LEVIN. Lieutenant General Alexander, do you support pilot projects and demonstrations to test out some of these ideas?

General ALEXANDER. [Deleted.]

12. Senator LEVIN. Lieutenant General Alexander, if the commercial telecommunications providers have the legal authority and capability to see cyber threats as they arise and traverse across the global network, they would be in a position to quickly identify where attacks originate, whereas the Government, as you have pointed out, must get warrants to start backtracking to trace the route of an attack. Is industry in principle in a better position to sense, characterize, and respond rapidly to threats in cyberspace?

General ALEXANDER. [Deleted.]

13. Senator LEVIN. Lieutenant General Alexander, which Government agency should manage a relationship with industry in which commercial-sector warning and threat information is provided to the Government? Should it be the Department of Homeland Security (DHS)?

General ALEXANDER. [Deleted.]

ADEQUACY OF NSA CYBER SECURITY SOLUTION

14. Senator LEVIN. Lieutenant General Alexander, Howard Schmidt, the President’s recently appointed cyber policy coordinator, just released a description of the equipment—known as Einstein 3—which NSA developed to help defend the military and Federal civilian networks from cyber attacks. He characterized it as a signatures-based intrusion detection and prevention system. Experts in cyber security, and leading security officials in DOD, believe that such intrusion prevention devices cannot by themselves defend against all threats, especially not certain kinds of sophisticated or unknown threats. DOD’s strategy is to include the Einstein 3 technology as one part of a defense-in-depth. Do you agree that Einstein 3 is but one element of a robust defensive capability?

General ALEXANDER. [Deleted.]

15. Senator LEVIN. Lieutenant General Alexander, do you think that the investments made to date under the Comprehensive National Cybersecurity Initiative, for non-DOD .gov agencies and departments, have reflected a proper balance between all the various aspects of a strong defense-in-depth?

General ALEXANDER. [Deleted.]

RESPONSE TO ATTACKS ON DOD NETWORKS

16. Senator LEVIN. Lieutenant General Alexander, in the advance policy questions, we asked you what the legal process is for backtracking through the layers of computers or servers located in the United States. Your reply was that law enforcement agencies have to do that, and they have to have a warrant. Then, if there are grounds at some point for believing that a foreign power is behind the attack that is routed through U.S. computers, a Foreign Intelligence Surveillance Act (FISA) warrant may be necessary. These procedures appear necessarily time-consuming—hardly matching the net speed that everyone touts as necessary.

We also asked you about the legality of shooting back against an attack that seems to come from U.S. sources, even if we cannot tell whether the attacking computers are the source of the attack, or whether they may have been commandeered for such as purpose.
Your answer is that the right to self defense allows commanders to return fire. Are you really saying that it is lawful and appropriate for U.S. military commanders to shoot back against computers located in the United States under the doctrine of self-defense—especially in light of the fact your answer to the first question was that a warrant is required to start to unravel the origins of an attack?

General ALEXANDER. Under normal circumstances, U.S. military forces would not be authorized to engage targets in the United States. However, the right and obligation of self-defense recognizes that under exceptional circumstances such a course of action may be justified. For example, if a military member comes under fire when guarding a military installation, even in the United States, the member is authorized to return fire in self-defense. There is no requirement for the member to hold fire and try to determine whether the attacker is a U.S. national. Similarly, in the cyber arena, when a military system comes under attack, the commander charged with protecting the system is authorized to act in self-defense. That right and obligation of self-defense may include cyber actions, which would be based on the severity of the attack, and could be characterized as “firing back” in order to stop the threat. Obviously, as in all military operations, the principles of necessity and proportionality would be applied. Military members would take care to use the minimally effective solution to stop the attack.

17. Senator LEVIN. Lieutenant General Alexander, how do you reconcile these answers?

General ALEXANDER. See answer to question #16.

18. Senator LEVIN. Lieutenant General Alexander, how could we ever get to a suitably rapid response to attacks that have been routed through U.S.-based computers and infrastructure if a complicated legal procedure is required?

General ALEXANDER. The challenge for U.S. cyber leadership is to balance the critical constitutional and legal protections we provide U.S. persons with the necessity of defending our Nation from attack. We must make use of every instrument of national power, drawing on the resources and authorities of every agency of our Government to prevent attacks on American interests. When prevention fails, we must have the clear authority to act swiftly to end adversary attacks. Working within the interagency process to determine how best to strike this balance is one of DOD’s top priorities.

REAL TIME REGIONAL GATEWAY PROGRAM

19. Senator LEVIN. Lieutenant General Alexander, an NSA Inspector General report on the Real Time Regional Gateway (RTRG) program found that the NSA SAE recommended to you in 2006 that the RTRG program be designated as a major acquisition, which would have subjected the program to a significantly higher degree of internal and external oversight. This recommendation was based on the fact that RTRG had grown immensely in size and scope and plans were being made to extend the fielding to multiple combatant commands. You rejected that recommendation and did not brief the USD(AT&L), even though you briefed the President, the Secretary of Defense, and other senior officials. Why did you not brief the USD(AT&L), and reject your SAE’s recommendation, in spite of the fact that you briefed the program to higher-level officials?

General ALEXANDER. [Deleted.]

QUESTIONS SUBMITTED BY SENATOR E. BENJAMIN NELSON

INTERAGENCY COOPERATION

20. Senator BEN NELSON. Lieutenant General Alexander, one thing that I commonly look for are stovepipes and whether the Services are duplicating efforts or truly enhancing overall mission effectiveness. Last year at the STRATCOM hearing, General Chilton highlighted the importance of sharing information among agencies, including the DHS, the Intelligence Community, and DOD, in addressing security risks in cyberspace. I worry that in response to cyber security threats, without strong coordination, agencies will create their own unique defenses. If each agency builds their own protective walls, they ultimately stifle collaboration and the ability to disseminate intelligence information among agencies, which has been our Achilles heel—an inability to share intelligence, connect the dots, and prevent future attacks. What do you see as your role in interagency coordination of cyber security and information exchange protocols?
General Alexander. I believe my role in interagency coordination of cyber security and information exchange protocols centers on improving mechanisms to foster this activity. Principal among these activities will be the collaboration/coordination across the operational cybersecurity centers such as NSA's NTOC, DHS's US–CERT, FBI's NCIJTF, JTF–GNO's JOC and others. Additional coordination efforts include to the Joint Interagency Task Force-Cyber (JIATF-Cyber) whose membership includes the NSA/Central Security Service, Defense Intelligence Agency, Central Intelligence Agency (CIA), Department of Justice, Federal Bureau of Investigation (FBI), Joint Warfare Analysis Center, Office of the Secretary of Defense/Joint Staff, Army, Navy, Air Force, Marine Corps, Joint Functional Component Command-Network Warfare (JFCC–NW), Joint Task Force-Global Network Operations (JTF–GNO), Joint Functional Component Command for Global Strike, Joint Information Operations Warfare Center (JIOWC), Departments of Treasury (DOT), State (DOS), and Homeland Security, and the combatant commands. As CYBERCOM matures, we will look to refine and improve our coordination processes with all our Cyber partners.

I believe my role must be as a proponent for improving the information exchange protocols among a variety of DOD and interagency partners every day. We need to do this not only through changes within our organizational structure and improvements to our procedures, but also through a change in organizational culture that fosters information sharing as essential to deterring our adversaries and preventing future attacks.


General Alexander. DISA is a DOD combat support agency that provides command and control capabilities and enterprise infrastructure to operate and assure a global net-centric enterprise in direct support of joint warfighters, national-level leadership, and other mission and coalition partners across the full spectrum of operations. A strong relationship between DISA and CYBERCOM is essential to ensure we build, lease, and/or operate networks so that they are defensible and so that we are able visualize a Common Operating Environment (COE) in cyberspace, which serves as a foundation for CYBERCOM's execution of delegated missions assigned to STRATCOM in the Unified Command Plan.

In recognition of the crucial nature of this relationship, the Director of DISA has committed to providing both a DISA Field Office to support CYBERCOM and a DISA Support Element, unique to CYBERCOM which will be integrated into the Joint Operations Center. CYBERCOM will provide a liaison officer to DISA to facilitate the exchange of information and coordination between the two commands.

22. Senator Ben Nelson. Lieutenant General Alexander, do you have or expect to have a formal process to provide requirements for DISA to use as it acquires future network systems?

General Alexander. [Deleted.]

23. Senator Ben Nelson. Lieutenant General Alexander, how will you ensure that DISA and the Service components' technical solutions to cyber security issues do not end up as proprietary solutions resulting in information stovepipes that limit our cyberspace operational effectiveness?

General Alexander. Technical capability development to support CYBERCOM mission needs will be driven by a formal requirements process, the definition and use of standards, and a force integration plan that will include the Service cyber components assigned to the command as well as DISA. Joint membership on a requirements review board will ensure that all entities participate in the identification, prioritization, and resource investment decisions for technical solutions. Close collaboration and joint status reviews among the respective development organizations will avoid duplication of effort, and ensure activities remain complementary whether developed by the Government or by industry. Supporting acquisition organizations must ensure the careful crafting of acquisition contracts and associated statements of work to ensure that the rare proprietary solution is not a stovepiped solution, but rather is fully integrated with cyber operations across the enterprise. If confirmed, we will work closely with STRATCOM, Joint Chiefs of Staff, Office of the Secretary of Defense, Acquisition, Technology, and Logistics, and the Military Departments to ensure these solutions are properly aligned and integrated.
24. Senator BEN NELSON. Lieutenant General Alexander, in February, Admiral Mullen stated before this committee that “Threats in cyberspace are increasing faster than our ability to adequately defend against them.” A key aspect of providing a strong cyber defense is having enough talented people with the right skills to do the job. The fiscal year 2010 budget increased the training capacity for cyber experts to attempt to improve the DOD’s ability to safeguard our information and information systems. What progress are the Services making in providing forces to address the cyber threat from a manning perspective?

General ALEXANDER. [Deleted.]

25. Senator BEN NELSON. Lieutenant General Alexander, is cyber training capacity sufficient to get out in front of this rapidly evolving threat? If not, what else is needed?

General ALEXANDER. [Deleted.]

26. Senator BEN NELSON. Lieutenant General Alexander, are the Services properly coordinating their cyber efforts such as training and material solutions to ensure we are adequately protected against the threat of a substantial cyber attack?

General ALEXANDER. The Services are leveraging existing mechanisms to coordinate training and material solutions to ensure our protection against cyber attacks, and I will continue to work closely with them on these efforts. The creation of CYBERCOM along with its Service cyber components should significantly enhance the efforts of the Services to train and equip cyber forces to a common standard.

Service initiatives to address cyber training shortfalls are well developed and coordinated. STRATCOM and NSA/CSS along with the Services have combined experience and expertise to confront the complicated issues related to Computer Network Operations (CNO) workforce development. Subject matter experts representing each of the CNO job functions have defined each work role, and outlined the knowledge, skills, abilities needed to perform those CNO tasks. Further enhancing this initiative are the combined efforts of the Consolidated Staff (JFCC–NW/JTF–GNO), under the auspices of STRATCOM and JFCOM, to develop a Cyber Training Initiative to assess combatant commander and Service joint cyber training efforts. Collectively, these efforts are ensuring our cyber training is coordinated among the Services and poised to address the threat of cyber attacks.

The Services’ continued use of the Joint Capabilities Integration and Development System (JCIDS) remains an essential element of coordinating material solutions to address our pressing cyber needs. These efforts—including capability needs, capability gap and non-materiel solutions—must continue. Concurrent with this, we will ensure the technical capability development to support CYBERCOM mission needs will be driven by a formal requirements process, and will include the Service cyber components.

QUESTIONS SUBMITTED BY SENATOR JAMES M. INHOFE

27. Senator INHOFE. Lieutenant General Alexander, I am convinced that DOD’s decision to stand up CYBERCOM is the right answer to a drastically growing threat. As you well know, there is a significant threat to our National security in the cyber world; a threat we are dealing with daily – attacks against our civilian and military infrastructure. Like threats to space assets, cyber threats fall into that nebulous realm of what is a direct attack and what is something just short of that. What are your thoughts on the seriousness of these threats?

General ALEXANDER. The adversaries our Nation faces today cover the full spectrum, from individual hackers to terrorists and organized criminal groups, as well as foreign militaries and intelligence services. Indeed, the growing cyber threat has outpaced our defenses, and we are experiencing increasingly sophisticated, coordinated, and damaging cyberpenetration. We face a dangerous combination of known—and unknown—vulnerabilities, strong adversary capabilities, and weak situational awareness that could compromise our personal and national security. Moreover, we have witnessed a dramatic rise over the past several years in the number of intrusions against our military networks; DOD networks are now scanned millions of times a day by unauthorized users. In the most serious and significant cyber incident to date on U.S. military computer networks, several thousand computers were infected by malicious software attempting to exploit military systems and compromise national security. These intrusions affected a number of critical systems re-
sponsible for military command and control. The seriousness of the threats our Na-
ation faces in cyberspace prompted the Secretary of Defense to stand up CYBERCOM
and ensure our military could maintain its ability to use cyberspace for critical mis-
sion operations. The interconnected nature of these networks will require
CYBERCOM to actively coordinate its operations both within the Department as
well as in close partnership with the other agencies authorized to address these
threats.

28. Senator INHOFE. Lieutenant General Alexander, what do we need to do to
combat these threats?
General ALEXANDER. [Deleted.]

29. Senator INHOFE. Lieutenant General Alexander, besides the charter of
CYBERCOM to address cyber-based threats, what else is within the CYBERCOM’s
purview?
General ALEXANDER. [Deleted.]

NETWORK/INTERNET SECURITY

30. Senator INHOFE. Lieutenant General Alexander, over the last decade, as inter-
net use and connectivity have become pervasive, most information technology (IT)
security spending that has been invested in “perimeter defense” of the “distributed
network”. Breaches seem frequent and sometimes seem easy, and therefore focusing
on IT security of the distributed network has been critical. While there has been
increasing focus and increasing spending on the IT security of the distributed net-
work over the past decade, I have been told that spending on IT security for the
mainframe network has declined. This could potentially lead to serious cyber security
vulnerabilities in our mainframe network. I have been told that DOD has created
and adhered to a strict set of security configuration controls for their mainframe
systems. However, there have been reports of classified Government systems being
breached. As I have been told in some detail, the peripheral security of networks
has been the primary focus with less effort spent on the mainframes. Does DOD
have any issues with its mainframe security, both in its air-gapped systems and in
the systems that are connected to the internet?
General ALEXANDER. [Deleted.]

31. Senator INHOFE. Lieutenant General Alexander, what is being done to secure
those networks and systems that are not Government or military but are critical
to us, such as civilian agencies, State governments, and private sector elements
such as utility companies, banks, pipelines, phone companies, et cetera?
General ALEXANDER. [Deleted.]

LAW AND CYBER COMMAND

32. Senator INHOFE. Lieutenant General Alexander, I just read a news release
from Defense News on the legal issues associated with our ability to conduct oper-
ations in cyber space. It basically said that the NSA can monitor when we are under
attack but right now DOD is powerless to respond due to DHS ownership of re-
sponding to network attacks. The article was not overly complimentary of the cur-
rent process. Experts indicated that we need to look at doing some serious review
of our statutory law. What are your thoughts on where we stand with the legal as-
pects of responding to cyber attacks?
General ALEXANDER. The process for DHS to request and receive DOD support for
any national event is known as Defense Support to Civil Authorities (DSCA). If
there is a national cyber emergency for which DOD assistance is requested, the Sec-
retary of Defense will provide guidance, and we will comply with such guidance
under all circumstances. Any DOD cyber assistance will partner with the U.S. Com-
puter Emergency Readiness Team (US-CERT), the DHS lead organization, under
their National Cyber Security Division, for the day-to-day defense of the Federal ex-
cutive branch (.gov) networks.
Separate from the DSCA process, however, a new legal framework may be needed
to ensure the cyber security of our Nation at large. President Obama’s Cyberspace
Policy Review specifically highlighted the mismatch between our technical capabili-
ties to conduct operations and the governing laws and policies for the United States.
As stated in the Cyberspace Policy Review, law applicable to cyberspace is a “com-
plex patchwork” that “shapes viable policy options.” This patchwork is the result of
the convergence of once very diverse industries and technologies—each governed by
different laws and policies—to create what we now call "cyberspace." In response to this convergence, “law and policy should continue to seek an integrated approach” that leverages all the capabilities and expertise of both the public and private sectors so that, together, we can enhance the national security, economic competitiveness, public safety and civil liberties and privacy of the American people. I completely agree with this finding.

Until this integrated approach can be realized, policy gaps exist that prevent us from doing all that can be done to increase the cyber security of the Nation, especially our Nation’s critical infrastructure. Foremost amongst these gaps are the potential impediments to the public-private cybersecurity information sharing partnership, which I believe is critical to more effectively attributing and counteracting this threat. These include two core issues. First, the U.S. Government needs to be able to disseminate to the owners of the critical infrastructure and other private sector entities threat information that reflects real time exigencies, and to receive such information from private entities, while balancing concerns regarding anti-trust regulations and other unfair competition matters; civil liberties and privacy; and due regard for the Constitution and all applicable laws, policies, and procedures. The second issue involves how private companies will protect sensitive Government information and use it for the purpose of better cybersecurity without incurring liability or unduly disrupting their network operations.

NSA/CSS, as a member of both DOD and the Intelligence Community and in partnership with DHS and other departments and agencies, is working closely with the President’s Cybersecurity Coordinator, Mr. Howard A. Schmidt, on these issues. We are exploring options within existing law, policy, and doctrine to address these issues and we will inform Congress if any legislation may be needed.

33. Senator INHOFE. Lieutenant General Alexander, what needs to be done to ensure that the bureaucracy does not interfere with our security necessities?

General ALEXANDER. In my experience, we currently have an unprecedented level of commitment across the public and private sectors to improving the cybersecurity of our Nation. Evidence of the commitment and cooperation is seen in the implementation of the Comprehensive National Cybersecurity Initiative (CNCI) and the President’s Cyberspace Policy Review. The issues the Nation faces in this domain are complex and challenging, necessarily taking time to thoughtfully resolve even with the complete commitment of all stakeholders. As stated in the Cyberspace Policy Review, integrating the Nation’s response to such challenging issues needs to be led “from the top,” which is happening under the leadership of Mr. Howard A. Schmidt, Special Assistant to the President and Cybersecurity Coordinator. In support of the Secretary of Defense, and if confirmed, I will continue to work to identify gaps, inform the development of meaningful and enduring national cyber policy, and be prepared to adjust rapidly to changes.

EDUCATION IN INFORMATION TECHNOLOGY

34. Senator INHOFE. Lieutenant General Alexander, when we met in my office yesterday, we discussed the need to attract extremely technical, qualified, and diverse professionals. This begins with ensuring our colleges and universities throughout the United States have programs in place to educate and groom future generations of IT professionals. One program we discussed was University of Tulsa’s iSec, specializing in educating students in cyber defense, deterrence, and warfare. Are we doing enough in academic institutions to produce the IT professionals this country needs in the future?

General ALEXANDER. We have seen a lot of progress in academic institutions responding to the high demand for IT professionals, but more can be done to build this critical resource. The explosion of cyber threats and increases in organized cyber crime activity has driven the trend for information technology professionals upward. We are starting to see more 4 year programs like the one at Tulsa and even 2 year programs at Community Colleges. For example, the Chronicle of Higher Education reported that as early as 7 years ago, virtually no Community Colleges offered cyber security programs. Now cyber security education has spread across the 2 year college sector, spurred by Federal grants and post-September 11 focus on infrastructure security. Finally, President Obama is stressing the importance of such colleges and a new White House cyber security push points to the need for workforce training. All of this demand does lead to an increasing role for 2 and 4 year colleges that can supply government agencies and private companies with workers steeped in cyber security.
Through partnerships with Government, academia, and industry, NSA’s Information Assurance (IA) Mission advocates improvements in IA education, training, and awareness. The National IA Education and Training Program (NIETP) operates as the national manager for IA education and training relating to national security systems. Its programs assure the very finest preparation of professionals entrusted with securing our critical information. The NIETP develops IA training standards with the Committee on National Security Systems. It also assesses current course IA offerings to identify gaps and determine how to fill those gaps. The NIETP encourages and recognizes universities through the National Centers of Academic Excellence in IA Education and the National Centers of Academic Excellence in Research. The NIETP is also one of the Government sponsors of the Colloquium for Information Systems Security Education. There are over 106 National Centers of Academic Excellence in the field of Information Assurance as recognized by the NSA/Central Security Service. Including The University of Tulsa’s iSec program, these institutes of higher learning are located in 37 different States, Washington, DC, and Puerto Rico. Prior to submitting an application for the National Center of Excellence Program, IA courseware must be certified under the IA Courseware Evaluation Program as meeting the Committee on National Security Systems (CNSS) Training Standards, and the certification must remain current. There is a minimum number of points required in nine different criteria to qualify as a National Center of Academic Excellence. The partnership that we have with all of these institutions of higher education will continue to evolve in order to meet the future need of producing the very best IT professionals. Through NSA and other government and industry efforts, we must remain engaged with academia to ensure we foster the development of the right curriculum, based on identifiable standards, to ensure the continued growth in the numbers of IT professionals our country will need in the future.

35. Senator INHOFE. Lieutenant General Alexander, is there a research/development gap in cyber defense/deterrence/technology/intelligence?

General ALEXANDER. There are research and development gaps that do exist in the areas of cyber operations and intelligence; principally these involve a need for shared situational awareness, better attribution technologies, and real-time visibility of intrusions into our networks. These and other gaps are being identified and used to influence DOD’s research and development priorities. The technical solutions associated with cyber defense will continue to evolve rapidly as our adversaries become increasingly sophisticated. Given that intrusions into DOD systems are virtually the same as those attacks experienced by the commercial sector, DOD can both benefit from and influence commercial development efforts, consistent with DOD authorities, to address those vulnerabilities. Ultimately, we believe automated solutions which adapt to rapidly increasing adversary capability sophistication and to employ proactive measures to defeat adversary attacks will be critical to ensuring the defense of our military networks.

STANDING UP CYBER COMMAND

36. Senator INHOFE. Lieutenant General Alexander, as I have seen with the standup of U.S. Africa Command (AFRICOM), putting together a combatant or functional command organization is a tall order. It requires herculean efforts on the parts of all entities and can easily be subjected to inertia and bureaucracy. What is your understanding of the infrastructure and capabilities requirements and status of CYBERCOM?

General ALEXANDER. [Deleted.]

37. Senator INHOFE. Lieutenant General Alexander, what is needed to ensure the command is fully functional?

General ALEXANDER. Since CYBERCOM will initially be established with the existing personnel from JFCC–NW and JTF–GNO along with existing military Service component organizations, I believe that we will be fully functional upon establishment of the command. That being said, if confirmed and upon activation, we will be looking to continually enhance and evolve our mission effectiveness. We need to build capacity (trained personnel, facilities, communications, IT . . . ), enable effective collaboration (DOD, interagency, government, industry, academia, foreign partners), and achieve collocation of a critical set of core capabilities to provide agility in defending known, emerging, and unanticipated threats. In the short term, we are standing up the headquarters within the Fort Meade area/NSA campus by merging the JTF–GNO and JFCC–NW mission sets to better leverage the capabilities of the
global SIGINT enterprise while using existing infrastructure. As necessary, we will pursue more contiguous space solutions to house our authorized strength, host key Service cyber component elements and liaison offices.

38. Senator INHOFE. Lieutenant General Alexander, what will be the interagency support to the headquarters?

General ALEXANDER. Currently, we have several representatives from key interagency partners integrated into the Consolidated JFCC–NW/JTF–GNO staff. My intent is to grow and strengthen these relationships by increasing the level of integration of our key interagency partners. As an example, we intend to further promote this enhanced coordination and collaboration by seeking the integration of interagency personnel on the CYBERCOM operations floor. We will also explore opportunities to expand DOD/NSA liaison positions at other key departments and agencies. In addition we will seek ways to improve the interagency coordination process under the command’s purview. One such process is the day-to-day operational planning, decision support, and coordination performed by JIATF-Cyber that coordinates offensive cyberspace operations. Current member organizations of JIATF-Cyber includes the NSA/Central Security Service, Defense Intelligence Agency, Central Intelligence Agency (CIA), Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Joint Warfare Analysis Center, Office of the Secretary of Defense/Joint Staff, Army, Navy, Air Force, Marine Corps, JFCC–NW, JTF–GNO, Joint Functional Component Command for Global Strike, JIOWC, Departments of Treasury (DOT), State (DOS), and Homeland Security and the combatant commands. As CYBERCOM matures, we will look to improve this process and expand our coordination to full-spectrum cyberspace operations.

39. Senator INHOFE. Lieutenant General Alexander, how will your responsibilities for the NSA impact or integrate with your responsibilities for CYBERCOM?

General ALEXANDER. Across my 41⁄2 years as the Director of NSA/Chief, CSS, and Commander of JFCC–NW (18 months of which I also served as the operational commander of JTF–GNO), I have worked closely with and been supported by excellent line commanders and leaders across the STRATCOM, NSA, and CSS organizations who, in turn, have taken on greater responsibility for executing their assigned tasks while ensuring greater synchronization with all. I fully expect to be able to draw upon the capabilities and talents of that broad leadership cadre combined with the additional leaders that will join us upon activation of CYBERCOM to effectively synchronize their work across NSA and CYBERCOM.

While CYBERCOM’s ability to leverage NSA’s cryptologic capabilities and its world class Information Assurance expertise will be critical to its success in operating in the cyber domain, CYBERCOM and NSA will remain separate and distinct organizations with their own identities, authorities, missions, funding, and oversight mechanisms. I intend to draw upon the extensive lessons I have learned over the past 41⁄2 years to ensure that I am able to perform both missions effectively. The addition of a three-star Deputy Commander for CYBERCOM, a fully resourced joint staff and robust Service cyber components will be critical enablers in this regard.

40. Senator INHOFE. Lieutenant General Alexander, where would you like to see CYBERCOM in the next 1, 5, and 10 years?

General ALEXANDER. Over the next year, I see CYBERCOM focusing on building the command and staff, implementing an effective operational construct; and informing, and benefiting from, the development of DOD’s policy and strategy review to address cyberspace operations. Building the command includes relocation of over 400 JTF–GNO personnel from Arlington to Fort Meade, the establishment of a joint staff structure, and the stand up of service cyber components. Implementing an effective operational construct is also key during the coming year and centers on improving our ability to dynamically defend our military networks as well as the development of a structured process to receive and respond to combatant command cyber requirements. Underlying all of these goals is the ongoing Under Secretary of Defense for Policy-led, review of DOD cyberspace policy. This effort, as it comes to fruition, will significantly shape and influence our actions in the cyber domain.

At year 5, I envision a significant improvement in defending our military cyber infrastructure. This improvement will be bolstered by substantive growth and maturation of our Service cyber capacity and capability as well as a considerable investment in physical and information technology infrastructure to support shared cyber situational awareness. Moreover, I envision a robust partnership with the DHS and commercial sector to ensure the defense of the .mil, .gov, and critical infrastructure, with roles, responsibilities and authorities clearly defined and executed. At year 10, I envision CYBERCOM, working closely with the Services, component commands,
and select agencies achieving a mature integrated operational construct that allows for seamless interoperability, a capability to conduct net-speed operations and a COE to conduct effective operations in cyberspace.

41. Senator INHOFE. Lieutenant General Alexander, what level of funding is necessary to achieve these goals?
   General ALEXANDER. [Deleted.]

QUESTIONS SUBMITTED BY SENATOR GEORGE S. LE MIEUX

42. Senator LE MIEUX. Lieutenant General Alexander, what threshold would constitute an act of war?
   General ALEXANDER. [Deleted.]

43. Senator LE MIEUX. Lieutenant General Alexander, would we be willing to commit kinetic forces in response to a cyber attack?
   General ALEXANDER. The President and the Secretary of Defense would determine whether kinetic forces were to be committed. Important considerations informing this decision would include the scale of the attack and the ability to attribute it to a specific adversary as well as the destructive effect. The use of kinetic force in response to a cyber attack would also need to satisfy necessity and proportionality requirements of the law of armed conflict.

44. Senator LE MIEUX. Lieutenant General Alexander, who are the decisionmakers in reacting and responding to a cyber attack?
   General ALEXANDER. [Deleted.]

45. Senator LE MIEUX. Lieutenant General Alexander, a March 23rd article in Defense News claims that 120 countries have or are developing offensive cyber attack capabilities. Is the United States prepared to deal with this threat?
   General ALEXANDER. While the majority of these nations developing offensive cyber attack capabilities are not our adversaries, the United States does in fact face a serious threat from a spectrum of actors. The growing cyber threat has, in fact and in my opinion, outpaced the country's defenses and we are experiencing increasingly sophisticated, coordinated, and damaging cyber penetration, for which I do not believe we are adequately prepared.

The ever increasing intrusions into our classified and unclassified military networks specifically, led to the Secretary of Defense's decision to establish CYBERCOM in order to confront the threats and reduce the vulnerability of our military cyber infrastructure. As recognized in the President's Cyberspace Policy Review, what is truly needed, however, is a comprehensive framework to ensure coordinated response and recovery by the whole of government working with the private sector. The interconnected nature of DOD networks and the free flow of information across various domains necessitate an active partnership between DOD and agencies across the U.S. Government, along with the private sector, to ensure that the security of these networks is synchronized. CYBERCOM will focus on securing the Nation's military networks. Military operations and command and control, however, no longer consistently fit neatly within the boundaries of the .mil networks. Increasingly, key logistics and other operational missions are performed by cleared defense contractors and commercial vendors via routine network communications. Thus, protecting the Nation's military networks and operations from disruption will increasingly require close interaction with such entities and new constructs to guarantee unimpeded operations.

As DOD works through the development of these new constructs, we will do so in concert with the White House, the Justice Department, DHS, and other agencies to ensure we develop a synchronized way ahead within an overall national cyber policy framework. These collective efforts will be foundational to our Nation's success in the cyber domain.

QUESTIONS SUBMITTED BY SENATOR DAVID VITTER

46. Senator VITTER. Lieutenant General Alexander, first, I want to thank you for our productive meeting and discussion last month about NSA's continuing oper-
General ALEXANDER. [Deleted.]

47. Senator VITTER. Lieutenant General Alexander, will you make offensive capabilities a priority to counter or deter other nations’ cyber attacks?

General ALEXANDER. [Deleted.]

QUESTIONS SUBMITTED BY SENATOR SUSAN COLLINS

GOVERNMENT/PRIVATE SECTOR COLLABORATION

48. Senator COLLINS. Lieutenant General Alexander, how critical is collaboration between the private sector and the Government to reducing our cyber vulnerabilities?

General ALEXANDER. Collaboration is absolutely essential. I believe building an effective partnership between the U.S. Government and the Nation’s private sector is integral to reducing the country’s cyber vulnerabilities.

Cyberspace is fundamentally owned and operated by the private sector. Most of the government infrastructure is owned and operated by private industry. For our mutual defense, the Government must share information and expertise regarding threats and vulnerabilities with the private sector—and the private sector should be able to do the same. It must be a partnership.

49. Senator COLLINS. Lieutenant General Alexander, can you discuss how the NSA and CYBERCOM currently interact with the private sector and your plans for that interaction to be stronger in the future?

General ALEXANDER. [Deleted.]

50. Senator COLLINS. Lieutenant General Alexander, what specific provisions in Federal law prevent information sharing between the Government and the private sector, thus hampering our efforts to protect cyberspace?

General ALEXANDER. [Deleted.]

51. Senator COLLINS. Lieutenant General Alexander, if the private sector shares information with the Government to help protect against criminal and terrorist attacks, are there adequate protections in place within the NSA and CYBERCOM to guard against the release of trade secrets and other proprietary information?

General ALEXANDER. [Deleted.]

CYBER COORDINATION

52. Senator COLLINS. Lieutenant General Alexander, NSA and CYBERCOM play lead roles in protecting U.S. military networks. DHS is the lead agency in terms of protecting the Federal Government’s civilian networks and the Nation’s critical infrastructure. How do you plan to coordinate the different responsibilities of NSA, CYBERCOM, and DHS in this regard?

General ALEXANDER. Each organization has specific missions and authorities, and all will be required in order to increase the cybersecurity of the Nation. Therefore, as you state, coordination is essential for success. In my experience, the elements of effective coordination are communication, collaboration, and respect. In response to cyber threats and intrusions already encountered NSA, the Joint Task Force for Global Network Operations (JTF–GNO) and DHS are continually strengthening coordination in a manner that recognizes and respects each others’ authorities and capabilities, supports the exchange of vital information, and results in collaboration on solutions that mitigate the threat and reduce vulnerabilities. DHS, NSA, and the Consolidated Staff (Joint Functional Component Command Network Warfare and JTF–GNO) have also conducted a series of table top exercises to improve coordination in cyberspace. Coordination, however, is necessary beyond these three organizations. Coordination with other key departments and agencies, to include the Federal Bureau of Investigation, the Department of State, and the Department of Justice, as well as State, local, and tribal government, industry and our allies is imperative.

In accordance with the White House Cyberspace Policy Review, the White House Cybersecurity Coordinator is leading this national effort. Secretary Gates directed the creation of CYBERCOM to establish a framework under which a single military command can achieve unity of command and oper-
ational integration within DOD across the full-range of cyberspace operations. CYBERCOM will increase the DOD's effectiveness in this critical domain.

53. Senator COLLINS. Lieutenant General Alexander, what is the NSA's role in forming the technical standards, guidelines, or best practices for protecting the evolving networks of the Government and the private sector?

General ALEXANDER. [Deleted.]

CYBER ATTACKS

54. Senator COLLINS. Lieutenant General Alexander, the former DNI, Mike McConnell, recently pronounced that the United States “is fighting a cyber war today and it is losing.” Various reports have indicated that foreign powers have been at the root of serious and malicious cyber attacks against U.S. Government networks and against private interests. The recently released Quadrennial Defense Review states that DOD’s networks “are infiltrated daily by myriad of sources, ranging from small groups of individuals to some of the largest countries in the world.” In many cases, the attacks have been conducted through private networks to cover their tracks. At what point does an attack by a foreign power on our Government’s systems or on a U.S. private sector system become an act of war?

General ALEXANDER. [Deleted.]

55. Senator COLLINS. Lieutenant General Alexander, authentication of the source of a cyber attack is a critical component of any response to the attack. However, authentication can often be a difficult undertaking in the area of cyber security. It often requires the cooperation of multiple Federal agencies as well as the assistance of foreign governments. What steps is CYBERCOM taking to address this challenge?

General ALEXANDER. [Deleted.]

56. Senator COLLINS. Lieutenant General Alexander, what actions should the U.S. Government take to improve authentication efforts, including the need to pass any new laws?

General ALEXANDER. We must approach this problem in several ways. First, we must continue to encourage collaboration within the Intelligence Community to improve our ability to determine authentication. Second, we must invest in the right technologies to promote rapid attribution of cyber intrusions as well as agile tipping and cueing mechanisms to provide early warning and rapid response to these threats. This must be done with careful attention to the protection of privacy and civil liberties; if we are successful, these measures and the resulting strengthening of cybersecurity will enhance privacy through better protection of private information.

It is not clear at this time whether new laws are required to improve U.S. Government authentication efforts, though some gaps do exist today that prevent us from using technology to its fullest to increase the cyber security of the nation, especially our Nation’s critical infrastructure. Foremost amongst these gaps are the potential impediments to the public-private cybersecurity information sharing partnership, which I believe is critical to more effectively attributing and countering this threat. These include two core issues. First, the U.S. Government needs to be able to disseminate to the owners of the critical infrastructure and other private sector entities threat information that reflects real time exigencies, and to receive such information from private entities, while balancing concerns regarding anti-trust regulations and other unfair competition matters; civil liberties and privacy; and due regard for the Constitution and all applicable laws, policies, and procedures. The second issue involves how private companies will protect sensitive government information and use it for the purpose of better cybersecurity without incurring liability or unduly disrupting their network operations.

NSA/CSS, as a member of both DOD and the Intelligence Community and in partnership with DHS and other departments and agencies, is working closely with the President’s Cyber Security Coordinator, Mr. Howard A. Schmidt, on these issues. We are exploring options within existing law, policy, and doctrine to address these issues and we will notify Congress if any legislation maybe needed.

[The nomination reference of LTG Keith B. Alexander, USA, follows:]
NOMINATION REFERENCE AND REPORT

AS IN EXECUTIVE SESSION,
SENATE OF THE UNITED STATES,
October 20, 2009.

Ordered, That the following nomination be referred to the Committee on Armed Services:
The following named officer for appointment in the U.S. Army to the grade of indicated while assigned to a position of importance and responsibility under title 10, U.S.C., section 601:

To be General.

LTG Keith B. Alexander, 9763.

[The biographical sketch of LTG Keith B. Alexander, USA, which was transmitted to the committee at the time the nomination was referred, follows:]

DEPARTMENT OF THE ARMY,
OFFICE OF THE CHIEF OF LEGISLATIVE LIAISON,

Hon. CARL LEVIN, Chairman,
Committee on Armed Services,
U.S. Senate,
Washington, DC.

DEAR MR. CHAIRMAN: The President has forwarded to you under separate cover the following nomination.

For appointment to the grade of General:
Lieutenant General Keith B. Alexander, Director, National Security Agency/Chief, Central Security Service, Fort Meade, MD, as Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command, Fort Meade, MD.

For the information of the committee, I am enclosing a military career resume for this officer showing his assignments and grades held.

Sincerely,

BERNARD S. CHAMPOUX,
Major General, U.S. Army,
Chief of Legislative Liaison.

Enclosure

TRANSCRIPT OF NAVAL SERVICE FOR LTG KEITH B. ALEXANDER, USA

Source of commissioned service: USMA.

Educational degrees:
U.S. Military Academy - BS - No Major
Boston University - MS - Business Administration
Naval Postgraduate School - MS - Electronic Warfare
Naval Postgraduate School - MS - Physics
National War College - MS - National Security Strategy

Military schools attended:
Armor Officer Basic Course
Military Intelligence Officer Advanced Course
U.S. Army Command and General Staff College
National War College

Foreign language(s): None recorded.

Promotions:

<table>
<thead>
<tr>
<th>Promotions</th>
<th>Date of appointment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2LT</td>
<td>5 Jun 74</td>
</tr>
<tr>
<td>1LT</td>
<td>5 Jun 76</td>
</tr>
<tr>
<td>CAPT</td>
<td>8 Aug 78</td>
</tr>
<tr>
<td>MAJ</td>
<td>1 Sep 85</td>
</tr>
<tr>
<td>LTC</td>
<td>1 Apr 91</td>
</tr>
</tbody>
</table>
Major permanent duty assignments:

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb. 75</td>
<td>Mar. 76</td>
<td>Platoon Leader, B Company, 2d Battalion, 81st Armor, 1st Armored Division, U.S. Army Europe and Seventh Army, Germany</td>
</tr>
<tr>
<td>Mar. 76</td>
<td>June 77</td>
<td>Assistant S–4 (Logistics), later S–4, 511th Military Intelligence Battalion, 68th Military Intelligence Group, U.S. Army Europe and Seventh Army, Germany</td>
</tr>
<tr>
<td>July 77</td>
<td>June 78</td>
<td>Commander, Field Office, 511th Military Intelligence Battalion, 68th Military Intelligence Group, U.S. Army Europe and Seventh Army, Germany</td>
</tr>
<tr>
<td>July 78</td>
<td>Feb. 79</td>
<td>Student, Military Intelligence Officer Advanced Course, U.S. Army Military Intelligence Center and School, Fort Huachuca, AZ</td>
</tr>
<tr>
<td>Feb. 79</td>
<td>July 79</td>
<td>Electronic Warfare Staff Officer, 525th Military Intelligence Group, Fort Bragg, NC</td>
</tr>
<tr>
<td>July 79</td>
<td>Jan. 81</td>
<td>Commander, 336th Army Security Agency Company, 319th Military Intelligence Battalion (Corps), Electronic Warfare Intelligence, 525th Military Intelligence Group, Fort Bragg, NC</td>
</tr>
<tr>
<td>Jan. 81</td>
<td>July 81</td>
<td>Assistant S–3 (Operations), 525th Military Intelligence Group, Fort Bragg, NC</td>
</tr>
<tr>
<td>Aug. 81</td>
<td>Sep. 83</td>
<td>Student, Naval Postgraduate School, Monterey, CA</td>
</tr>
<tr>
<td>Oct. 83</td>
<td>June 85</td>
<td>Operations Officer, later, Chief, Intelligence Electronic Warfare Systems Task Force, later, Chief, Concepts and Studies Division, U.S. Army Intelligence Center and School, Fort Huachuca, AZ</td>
</tr>
<tr>
<td>June 85</td>
<td>June 86</td>
<td>Student, U.S. Army Command and General Staff College, Fort Leavenworth, KS</td>
</tr>
<tr>
<td>June 86</td>
<td>June 88</td>
<td>Deputy Director, Intelligence and Electronic Warfare Master Plan Special Task Force, later Intelligence Staff Officer, Office of the Deputy Chief of Staff for Intelligence, U.S. Army, Washington, DC</td>
</tr>
<tr>
<td>Jun 88</td>
<td>Mar. 90</td>
<td>S–3 (Operations), later Executive Officer, 522d Military Intelligence Battalion, 2d Armored Division, Fort Hood, TX</td>
</tr>
<tr>
<td>Mar. 90</td>
<td>June 91</td>
<td>Assistant Chief of Staff, G–2 (Intelligence), 1st Armored Division, U.S. Army Europe and Seventh Army, Germany and Operations Desert Shield/Storm, Saudi Arabia</td>
</tr>
<tr>
<td>June 91</td>
<td>July 93</td>
<td>Commander, 204th Military Intelligence Battalion, U.S. Army, Europe and Seventh Army, Germany</td>
</tr>
<tr>
<td>Aug. 93</td>
<td>June 94</td>
<td>Student, National War College, Fort McNair, Washington, DC</td>
</tr>
<tr>
<td>June 94</td>
<td>May 95</td>
<td>Chief, Army Intelligence Initiatives, Office of the Deputy Chief of Staff for Intelligence, U.S. Army, Washington, DC</td>
</tr>
<tr>
<td>May 95</td>
<td>June 97</td>
<td>Commander, 525th Military Intelligence Brigade, Fort Bragg, NC</td>
</tr>
<tr>
<td>June 97</td>
<td>July 98</td>
<td>Deputy Director for Intelligence, J–2, The Joint Staff (Defense Intelligence Agency), Washington, DC</td>
</tr>
<tr>
<td>July 98</td>
<td>Feb. 01</td>
<td>Director for Intelligence, J–2, U.S. Central Command, MacDill Air Force Base, FL</td>
</tr>
<tr>
<td>Feb. 01</td>
<td>July 03</td>
<td>Commanding General, U.S. Army Intelligence and Security Command, Fort Belvoir, VA</td>
</tr>
<tr>
<td>Aug. 03</td>
<td>July 05</td>
<td>Deputy Chief of Staff, G–2, U.S. Army, Washington, DC</td>
</tr>
<tr>
<td>Aug. 05</td>
<td>Present</td>
<td>Director, National Security Agency/Chief, Central Security Service, Fort Meade, MD</td>
</tr>
</tbody>
</table>

Summary of joint assignments:

<table>
<thead>
<tr>
<th>Date</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar. 90–June 91</td>
<td>Lieutenant Colonel</td>
</tr>
<tr>
<td>June 97–July 98</td>
<td>Colonel</td>
</tr>
<tr>
<td>July 98–Feb. 01</td>
<td>Brigadier General</td>
</tr>
<tr>
<td>Aug. 05–Present</td>
<td>Lieutenant General</td>
</tr>
</tbody>
</table>

Summary of operations assignments:

<table>
<thead>
<tr>
<th>Date</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar. 90–June 91</td>
<td>Lieutenant Colonel</td>
</tr>
</tbody>
</table>

U.S. decorations and badges:
Distinguished Service Medal (with two Oak Leaf Clusters)
Defense Superior Service Medal (with Oak Leaf Cluster)
Legion of Merit (with four Oak Leaf Clusters)
Bronze Star Medal
Meritorious Service Medal (with four Oak Leaf Clusters)
Air Medal
Army Commendation Medal (with Oak Leaf Cluster)
Army Achievement Medal (with Oak Leaf Cluster)
Senior Parachutist Badge
Joint Chiefs of Staff Identification Badge
Army Staff Identification Badge

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

UNITED STATES SENATE
COMMITTEE ON ARMED SERVICES
Room SR–228
Washington, DC 20510–6050
(202) 224–3871

COMMITTEE ON ARMED SERVICES FORM
BIOGRAPHICAL AND FINANCIAL INFORMATION REQUESTED OF NOMINEES

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

PART A—BIOGRAPHICAL INFORMATION

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

1. Name: (Include any former names used.)
Keith B. Alexander.

2. Position to which nominated:
Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command.

3. Date of nomination:
October 20, 2009.

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

5. Date and place of birth:
December 2, 1951; Syracuse, NY.

6. Marital Status: (Include maiden name of wife or husband’s name.)
Married to Deborah Lynn Alexander (nee Douglas).

7. Names and ages of children:
Jennifer Lynn Leonard, age 33.
Julie Marie Bailey, age 31.
Diana Lauri Glaser, age 29.
Heather Michelle Burton, age 25.

8. Government experience: List any advisory, consultative, honorary, or other part-time service or positions with Federal, State, or local governments, other than
those listed in the service record extract provided to the committee by the executive branch.

None.

9. **Business relationships:** List all positions currently held as an officer, director, trustee, partner, proprietor, agent, representative, or consultant of any corporation, company, firm, partnership, or other business enterprise, educational, or other institution.

None.

10. **Memberships:** List all memberships and offices held in professional, fraternal, scholarly, civic, business, charitable, and other organizations.

   Association of U.S. Army.

11. **Honors and awards:** List all scholarships, fellowships, honorary society memberships, and any other special recognitions for outstanding service or achievements other than those listed on the service record extract provided to the committee by the executive branch.

   None.

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

   Yes.

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

   Yes.

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

---

**Signature and Date**

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

Keith B. Alexander.

This 1st day of July, 2009.

[The nomination of LTG Keith B. Alexander, USA, was reported to the Senate by Chairman Levin on May 5, 2010, with the recommendation that the nomination be confirmed. The nomination was confirmed by the Senate on May 7, 2010.]