HEARING TO RECEIVE TESTIMONY ON U.S. STRATEGIC COMMAND AND U.S. CYBER COMMAND IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST FOR FISCAL YEAR 2013 AND THE FUTURE YEARS DEFENSE PROGRAM

TUESDAY, MARCH 27, 2012

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

The committee met, pursuant to notice, at 9:33 a.m. in room SD–106, Dirksen Senate Office Building, Senator Carl Levin (chairman) presiding.

Committee members present: Senators Levin, Lieberman, Reed, Nelson, Webb, Udall, Hagan, Manchin, Shaheen, Gillibrand, Blumenthal, McCain, Inhofe, Sessions, Chambliss, Ayotte, and Collins.

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

Majority staff members present: Joseph M. Bryan, professional staff member; Jonathan S. Epstein, counsel; Richard W. Fieldhouse, professional staff member; and Thomas K. McConnell, professional staff member.

Minority staff members present: Ann E. Sauer, minority staff director; Daniel A. Lerner, professional staff member; and Michael J. Sistak, research assistant.

Staff assistants present: Jennifer R. Knowles, Hannah I. Lloyd, and Bradley S. Watson.

Committee members' assistants present: Carolyn Chuhta, assistant to Senator Reed; Ryan Ehly, assistant to Senator Nelson; Gordon Peterson, assistant to Senator Webb; Casey Howard, assistant to Senator Udall; Mara Boggs, assistant to Senator Manchin; Elana Broitman, assistant to Senator Gillibrand; Ethan Saxon, assistant to Senator Blumenthal; Clyde Taylor IV, assistant to Senator Chambliss; Charles Prosch, assistant to Senator Brown; Brad Bowman, assistant to Senator Ayotte; and Rob Epplin, assistant to Senator Collins.

OPENING STATEMENT OF SENATOR CARL LEVIN, CHAIRMAN

Chairman LEVIN. Good morning, everybody.

Today's hearing continues a series of posture hearings that the Armed Services Committee is conducting on our combatant commands within the context of the fiscal year 2013 budget request and the President's new Strategic Guidance. Today we receive testimony from the U.S. Strategic Command and the U.S. Cyber Command, a sub-unified command of the U.S. Strategic Command.

Let me first welcome General Robert Kehler, the Commander of the U.S. Strategic Command, and General Keith Alexander, the Commander of the U.S. Cyber Command, and thank them both for their service to our Nation.

We also want to thank the fine men and women who serve in these commands for their dedication and service to our Nation and a special thanks to their families.

Strategic Command, or STRATCOM, manages nine missions across the Department of Defense. These missions range from satellite and space situational awareness, missile defense, and electronic warfare, to combating weapons of mass destruction. STRATCOM coordinates the activities of the U.S. Cyber Command across the Department of Defense. Unlike combatant commands which are regionally focused, STRATCOM's missions are global.

As noted in the President's Strategic Guidance, STRATCOM commands "nuclear forces that can under any circumstances confront an adversary with the prospect of unacceptable damage." That capability needs to be preserved as we continue to reduce the size of these forces and modernize the infrastructure at the Department of Energy that supports this mission.

General Kehler, here are some of the issues that I hope that you will address this morning.

First, are you satisfied with the direction that we are taking in our nuclear force posture and with the Department of Energy's role in maintaining our nuclear stockpile so that we can continue to reduce its size without testing while ensuring the stockpile remains safe and meets military requirements?

Second, do you believe we are on a sustainable path to protect our space assets and to reconstitute them, if necessary, given the congested and contested nature of space?

Third, the Department of Defense is allocated a block of the electromagnetic spectrum that connects our space, cyber, and electronic warfare assets to our forces. STRATCOM is the lead combatant command for synchronizing spectrum operations. How concerned are you about the prospect of losing spectrum and what are you doing to preserve the Department's access to it?

Fourth, with the cancelation of the Operationally Responsive Space program, are you worried about our ability to field low-cost but rapidly deployable satellites that can fill capability gaps between large national intelligence satellite collection systems and the Department's airborne surveillance platforms?

Fifth, what is your strategic vision for the combined use of space and cyber? These two domains are integrally linked but we have not seen a plan for integrating capabilities and operations.

Let me now turn to Cyber Command for a moment.

There is much for us to examine in this increasingly important and complex, but still new mission area, not only as it affects the Department of Defense, but the Government and the economy as a whole.

General Alexander has stated that the relentless industrial espionage being waged against U.S. industry and Government chiefly by China constitute "the largest transfer of wealth in history." The committee needs to understand the dimensions of this technology theft and its impact on our national security and prosperity.

The Armed Services Committee has focused for some time on the need to develop comprehensive policies and frameworks to govern planning and operations in cyberspace. What are the rules of engagement if we are attacked by another nation, what is the doctrine for operations, and deterrence, and warfighting strategies. The administration has made progress in these areas, as reflected in recent strategy statements and in the development of comprehensive legislation to improve cybersecurity. But much more needs to be done.

As a still-developing sub-unified combatant command, the committee needs to understand the current and planned relationships between Cyber Command and STRATCOM and the other combatant commands. The Defense Department is considering the establishment of component cyber commands at the combatant commands. We need to know what command arrangements would apply to these potential components, as well as the authorities and the missions that STRATCOM has delegated to Cyber Command and those that it plans to retain.

General Alexander has stated publicly that he believes he needs additional authorities to defend the networks and information systems of the rest of the Federal Government and those of critical infrastructure. The committee needs clarity on exactly what authorities General Alexander might be seeking and whether they go beyond what the administration has requested in its legislative proposal to Congress.

General Alexander has also often stated that the Department of Defense does not, in fact, have a unified network but rather 15,000 separate networks or enclaves into which Cyber Command has little visibility. The committee needs to understand what can and should be done to correct what would seem to be an urgent and critical problem.

The Department of Defense has conducted a pilot program with a number of major companies in the defense industrial base, or DIB as it is called, and multiple Internet service providers, or ISPs, like AT&T and Verizon. Under that pilot program, the NSA provides signatures of known cyber penetration tools and methods directly to the DIB companies or to the ISPs that provide the DIB companies their communications services. The companies then use these signatures to detect and block intrusion attempts.

Carnegie Mellon conducted an independent assessment of the DIB pilot for DOD and concluded that NSA provided few signatures that were not already known to the companies themselves, and in many cases, the DIB companies by themselves detected advanced threats with their own non- signature-based detection methods that probably is not known to the NSA. And so we need to hear from General Alexander on his view of those issues as well.

We thank you both again for your service, for being here this morning.

And we call on Senator McCain.

[The prepared statement of Chairman Levin follows:]

STATEMENT OF SENATOR JOHN McCAIN

Senator McCAIN. Well, thank you, Mr. Chairman.

Let me thank our distinguished witnesses for joining us this morning and for their many years of service to our Nation.

U.S. Strategic Command is in the midst of pivotal change as we proceed with the modernization of the nuclear weapons complex and the nuclear triad and further embed cyberdefense and cyberattack in the core mission competencies of 21st century warfare.

On nuclear modernization, I am encouraged that even with the unprecedented level of defense spending uncertainty, the Department has maintained its commitment to modernizing the triad of nuclear delivery vehicles. Unfortunately, the same cannot be said for the National Nuclear Security Administration and their proposal to abandon or delay key elements of the nuclear weapons complex modernization plan. Ratification of the New START treaty was conditioned on a commitment by the President to modernize the weapons complex. Modernization is universally recognized as essential to the future viability of the nuclear weapons complex and a prerequisite for future reductions. It has now been over a year since the treaty entered into force, and we do not see any sign of the administration keeping those commitments.

Core to the Strategic Command mission is deterrence. However, as the frequency, sophistication, and intensity of cyber-related incidents continues to increase, it is apparent that this administration's cyber deterrence policies have failed to curb those malicious actions. The current deterrence framework, which is overly reliant on the development of defensive capabilities, has been unsuccessful in dissuading cyber-related aggression. Whether it is a nation state actively probing our national security networks, a terrorist organization seeking to obtain destructive cyber capabilities, or a criminal network's theft of intellectual property, we must do more to prevent, respond to, and deter cyberthreats. The inevitability of a large-scale cyberattack is an existential threat to our Nation, and a strategy overly reliant on defense does little to influence the psychology of attackers who operate in a world with few, if any, negative consequences for their actions.

Last July, General Cartwright, the former Vice Chairman of the Joint Chiefs of Staff, criticized the administration's reactive Strategy for Operating in Cyberspace saying, "If it's okay to attack me and I'm not going to do anything other than improve my defenses every time you attack me, it's very difficult to come up with a deterrent strategy." I look forward to hearing from our witnesses if they believe that a strategy overly focused on defense is sustainable and whether they agree more must be done to deter and dissuade those who look to hold U.S. interests at risk via cyberspace.

The Senate will soon begin debate on cybersecurity legislation. The central themes in that debate will focus on how to improve information sharing across the spectrum and whether a new Government bureaucracy will improve our cybersecurity. I have proposed legislation, the SECURE Act, that first focuses on removing legal hurdles that hinder information sharing rather than adding regulations that would shift focus and previous resources away from the actual cyberthreat. If a timely response is essential, how would another layer of bureaucratic red tape be helpful?

While the SECURE Act does not give new authorities to the National Security Agency or U.S. Cyber Command, few will deny that those institutions, not the Department of Homeland Security, are most capable of guarding against cyberthreats. Unfortunately, other legislative proposals favor prematurely adding more Government bureaucracy rather than focusing on accomplishing the objective of protecting our cyber interests.

General Alexander, during an FBI-sponsored symposium at Fordham University, you stated that if a significant cyberattack against this country were being planned, there may not be much that either Cyber Command or NSA could legally do to discover and thwart such an attack in advance. You said: "In order to stop a cyberattack, you have to see it in real time and you have to have hose authorities. Those are the conditions we've put on the table. Now how and what Congress chooses, that'll be a policy decision." In a fight where the threat can materialize in milliseconds and quick action is essential, I look forward to better understanding what authorities you believe are needed to protect United States interests both at home and abroad.

The Department of Defense is requesting nearly $3.4 billion for cybersecurity in fiscal year 2013 and almost $17.5 billion over the future years defense program. The cyber budget is one of the only areas of growth in the DOD budget because of broad agreement that addressing the cyberthreat must be among our highest priorities.

I thank the witnesses for appearing before the committee today and look forward to their testimony.

Thank you, Mr. Chairman.

[The prepared statement of Senator McCain follows:]

Chairman LEVIN. Thank you very much, Senator McCain.

Senator Kehler? I mean General Kehler. Excuse me.

STATEMENT OF GEN. C. ROBERT KEHLER, USAF, COMMANDER, U.S. STRATEGIC DEFENSE

General KEHLER. Thank you, Mr. Chairman. If it is okay with you, I would like to have my statement admitted to the record.

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

General KEHLER. Sir, Senator McCain, and distinguished members of the committee, thanks for this opportunity to present my views on U.S. Strategic Command's missions and priorities.

I am very pleased to be here today with General Keith Alexander, Cyber Command's Commander, and of course, as both of you have pointed out, cyber is a critical component of our global capabilities.

Without question, Mr. Chairman, we continue to face a very challenging global security environment marked by constant change, enormous complexity, and profound uncertainty. Indeed, change and surprise have characterized the year that has past since my last appearance before this committee. Over that time, the men and women of Strategic Command have participated in support of operations in Libya and Japan, have supported the withdrawal of

U.S. combat forces from Iraq, and have observed the Arab Spring, the bold operation that killed Osama bin Laden, the death of Kim Jong Il, and the succession of Kim Jong Un, growing violence in Syria, continued tensions with Iran, the passage of the Budget Control Act, and the adoption of new defense Strategic Guidance.

Through this extraordinary period of challenge and change, STRATCOM's focus has remained constant: to partner with the other combatant commands; to deter, detect, and prevent attacks on the United States, our allies and partners; and to be prepared to employ force, as needed, in support of our national security objectives. Our priorities are clear: deter attack, partner with the other commands to win today, respond to the new challenges in space, build cyberspace capability and capacity, and prepare for uncertainty. Transcending all of these priorities is the threat of nuclear materials or weapons in the hands of violent extremists.

And we do not have a crystal ball at STRATCOM, but we believe events of the last year can help us glimpse the type of future conflict that we must prepare for. Conflict will likely be increasingly hybrid in nature, encompassing all domains, air, sea, land, space, and cyberspace. It will likely cross traditional geographic boundaries, involve multiple participants, and be waged by actors wielding combinations of capabilities, strategies, and tactics. I think it is important to note the same space and cyberspace tools that connect us together to enable global commerce, navigation, and communication also present tremendous opportunities for disruption and perhaps destruction.

Just last month, the Department of Defense released new Strategic Guidance to address these challenges. This new guidance describes the way ahead for the entire DOD, but I believe many portions are especially relevant to STRATCOM in our broad assigned responsibilities.

For example, global presence, succeeding in current conflicts, deterring and defeating aggression, including those seeking to deny our power projection, countering weapons of mass destruction, effectively operating in cyberspace, space, and across all other domains, and maintaining a safe, secure, and effective nuclear deterrent, are all important areas in the new strategy where STRATCOM's global reach and strategic focus play a vital role.

No question these are important responsibilities. There are real risks involved in the scenarios we find ourselves in today. It is my job to prepare for those events and to advocate for the sustainment and modernization efforts we need to meet the challenges. In that regard, the fiscal year 2013 budget request is pivotal for our future. We are working hard to improve our planning and better integrate our efforts to counter weapons of mass destruction. We need to proceed with planned modernization of our nuclear delivery and command and control systems. We need to proceed with life extension programs for our nuclear weapons and modernize the highly specialized industrial complex that cares for them. We need to improve the resilience of our space capabilities and enhance our situational awareness of this increasingly congested, competitive, and contested domain. We need to improve the protection and resilience of our cyber networks, enhance our situational awareness, increase our capability and capacity, and work across the interagency to increase the protection of our critical infrastructure. We need to enhance our ISR capabilities. We need to better manage and synchronize the crucial processing, exploitation, and dissemination capabilities that support them. We need to get better at electronic warfare. We need to practice how to operate in a degraded space and cyberspace environment. We need to improve our understanding of our adversaries. We need to review our plans and improve our decision processes and command relations, all subjects that the two of you touched on in your opening comments.

In short, the new national security reality calls for a new strategic approach that promotes agile, decentralized action from a fully integrated and, I would say, fully interdependent and resilient joint force. These are tough challenges, but the men and women of STRATCOM view our challenges as opportunities, a chance to partner with the other commands to forge a better, smarter, and faster joint force.

We remain committed to work with this committee, the Services, other agencies, and our international partners to provide the flexible, agile, and reliable strategic deterrence and mission assurance capabilities that our Nation and our friends need in this increasingly uncertain world.

Mr. Chairman, it is an honor and a privilege to lead America's finest men and women. They are our greatest advantage. I am enormously proud of their bravery and sacrifice, and I pledge to stand with them and for them to ensure we retain the best force the world has ever seen. And in that, I join with the Secretary of Defense and the Chairman of the Joint Chiefs of Staff and other senior leaders, my colleagues, the other combatant commanders in thanking you for the support you and this committee have provided them in the past, present, and on into the future.

Before I close, Mr. Chairman, I would like to pause and remind the committee that STRATCOM is headquartered in the great State of Nebraska, and I wanted to take this opportunity to thank Senator Ben Nelson for his service. Senator Nelson will retire at the end of this Congress, and during his service, he has worked diligently to better the lives of our troops and to improve America's strategic forces. Those who live and work at Offutt Air Force Base are well aware of his deep commitment to them. So on behalf of your fellow Nebraskans at STRATCOM, Senator, we offer our thanks.

And with that, Mr. Chairman, thank you for this opportunity, and I look forward to your questions.

[The prepared statement of General Kehler follows:]

Chairman LEVIN. Thank you very much, General, and thank you for your reference to General Ben Nelson. Now I call him a General and you a Senator. To Senator Ben Nelson. We all feel very much the way you do, and we are grateful for your reference to him. Thank you.

General Alexander?

STATEMENT OF GEN KEITH B. ALEXANDER, USA, COMMANDER, U.S. CYBER COMMAND, AND DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE

General ALEXANDER. Chairman Levin, Ranking Member McCain, and distinguished members of the committee, thank you for the opportunity to appear before you today. I am pleased to appear with General Bob Kehler, and I echo his comments all across the board, including with Senator Nelson.

I would start up front by echoing some of those comments, which is it is a privilege and honor to lead the soldiers, sailors, airmen, marines, and civilians of Cyber Command and NSA. We have great people. Thanks for what you do to get those great people for us.

I would also like to thank you and your colleagues for your support in helping this command move rapidly forward in our efforts to address emerging threats and concerns to our Nation.

I also need to thank all our partners throughout DOD, DHS, and the FBI. We endeavor to build capability and capacity. Cyber is a team sport, and we could not have come this far and accomplished this much as we have without them.

Many changes and substantial progress have been made since I last spoke to the committee almost 2 years ago. Cyberspace has increasingly become more critical to our national and economic security. And, Chairman, you brought up one of the quotes about the greatest transfer of wealth. I think that is absolutely correct. We are seeing increased exploitation into industry, other Government agencies, and the theft of intellectual property is astounding. I will address parts of that shortly in my comments coming up.

I also think that the threat has grown in terms of activists, nation states, and non-nation state actors. The Secretary of Defense and chairman both emphasized cyber as an area of investment and a leaner defense budget. The task of assuring cyberspace access and security has drawn the attention of all our Nation's leadership. The U.S. Cyber Command is a component of a larger U.S. Government-wide effort to make cyberspace, one, safer and a forum for vibrant citizen interaction to preserve our freedom to act in cyberspace and defend our vital interests and those of our allies.

Cyber Command is charged to direct the security, operations, and defense of the Department of Defense information systems. But our work is affected by threats outside DOD's networks, threats the Nation cannot ignore. What we see both inside and outside DOD information systems underscores the imperative to act now to defend America in cyberspace.

The American people expect broad and efficient access to cyberspace. The military and civilian sectors rely on accessibility. Increased interconnectedness of information systems, growing sophistication of cyber criminals and foreign intelligence actors has increased our risk.

Last spring, in his international strategy for cyberspace, the President confirmed an inherent right to protect ourselves against attacks in this domain as in traditional domains. He said: When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. Cyber Command exists to ensure the President can rely on the DOD information systems and has military options available to defend our Nation.

The President and the Secretary of Defense recently reviewed our Nation's strategic interests, issued guidance on defense priorities. In sustaining U.S. global leadership, priorities for 21st century defense, the Secretary focused on protecting access throughout the cyber domain. The U.S. Cyber Command role is to pay attention to how nations and non-nation state actors are developing asymmetric capabilities to conduct cyber espionage and attacks. DOD recently added detail to that position. In accordance with the President's strategy, the Department further explained our deterrent posture to Congress in its cyberspace policy report last November.

DOD components, especially Cyber Command, work to dissuade others from attacking or planning to attack the United States in cyberspace. We work with a range of partners, U.S. Government allies, private industry to strengthen the defense of our citizens, the Nation, and allies in cyberspace. I want to assure you that all of our work is performed to safeguard the privacy and civil liberties of U.S. persons. These responsibilities are very much on our minds.

In establishing the COCOM relationships, you asked about our relationships with the other commands, and I would like to briefly address that.

First, we are establishing a cyber support element at each of the six geographically based COCOMs. CENTCOM's cyber support element is up and operational. PACOM's cyber support element is partially operational, and the others are on their way.

The purpose is to provide technical expertise and capability and improve integration of cyber capabilities into the COCOM mission planning efforts. Our goal is to ensure each COCOM has a full sweep of cyber operations to choose from and an understanding of effects these options can produce in their AOR.

Chairman, you also asked about the standing rules of engagement. The Department is conducting a coordinated, thorough review with the Joint Staff of existing standing rules of engagement on cyberspace. These revised standing rules of engagement should give us authorities we need to maximize pre-authorization of defense responses and empower activity at the lowest level. Issues being ironed out are what specific set of authorities we will receive, conditions in which we can conduct response actions, and we expect that those will be done in the next few months.

DOD's role in defense against cyberattacks. Defending the Nation in cyberspace requires coordination with several key Government players, notably DHS, the FBI, the intelligence community. I would just like to put some of this on the table because it is my opinion that we need all three working together as a joint team. DHS has the lead for coordinating the overall national effort to enhance cybersecurity of U.S. critical infrastructure. They lead in resilience and preparing the defense. The FBI has the lead for detection, investigation, prevention, and mitigation response within the domestic arena under their authorities for law enforcement, domestic intelligence, counterintelligence, and counterterrorism. And of course, DOD, NSA, and Cyber Command lead for detection, prevention, and defense in foreign space, defense of the Nation if the Nation comes under attack.

I would like to go into, if I could, a little bit on what I see we need in cyberspace, the requirements to defend the Nation from attack because there has been a lot of discussion on this, and I think it is important to put this up front. I think this is the heart of some of the discussion that is going on with the legislation today.

First, we need to see the attack. What do I mean by that? And that was a quote that we have made up at the Fordham University. If we cannot see the attack, we cannot stop it. What we are not talking about is putting NSA or the military into our networks to see the attack. What we are talking about that all of you put on the table is we have to have the ability to work with industry, our partners, so that when they are attacked or they see an attack, they can share that with us immediately. The information sharing and the liability that goes along would allow industry, armed with signatures that we can provide, signatures that they have—I agree it takes all of us working together—to provide a better defense. What we need is for them to tell us that something is going on.

There are a couple of analogies that I would like to use. These are not perfect analogies, just the best that I can come up with. Being in the Armed Services Committee here, I use the missile analogy.

So if a missile were coming into the country and we had no radars to see it, we could not stop that missile. If we have a cyberattack coming in and no one tells us that that cyberattack is going on, we cannot stop it.

Today, we are in the forensics mode. What that means is an attack or an exploit normally occurs. We are told about it after the fact. I think we should be in the prevention mode in stopping that. A lot of that can be done by industry. I think that industry should have the ability to see these and share that with Government in real time.

When you think about it, it is almost like the Neighborhood Watch program. Somebody is breaking into a bank. Somebody needs to call the authorities to stop it. In cyberspace, what we are saying is armed with the signatures, the malicious software, those things that help us understand that an attack is going on, we believe that industry is the right one to tell the Government that they see that and get us to respond to it.

So I just want to clarify it because I do not believe we want NSA or Cyber Command or the military inside our networks watching it. We think industry can do that, and we think that is the right first step. Actually that is in both of these bills.

The second part. I used that bank one because I think there is another part to this that we have in force within DOD, and that is what standards do we build our networks to and how much of a defense do we put in there. How do we make our defense better? So we have put in a series of defensive capabilities, if you will, the standards that we operate and defend our networks. How do you align your networks? How do you know that they are configured right? How do you make them defensible so that they will last when somebody is trying to get in?

We have a great Information Assurance Directorate, and one of the former directors told me that 80 percent of the exploits and attacks that come in could be stopped just by the hygiene itself.

Mr. Chairman, you also brought up the issue of the Carnegie Mellon report, and I would like to just hit some of that because I do think that is an important report and it really applies to this discussion that we have going on now.

As I have stated previously, that report and that assessment was early on in the DIB pilot. That does not mean that we cannot do better. In fact, let me turn that around and say for us to be successful in cyberspace, it is going to require Government and industry working together with the best of both. Industry partners see signatures that Government does not see, and government sees signatures or malicious software, exploitations, and attacks into the country that industry does not see. The information sharing and the ability to do that is key to stopping that.

What I see from the DIB pilot was increased discussion between Government and industry. And this was a good thing and it has grown and it continues to grow and we are getting better.

And so in legislation what I think is we need to make the first step. We need to start on that journey. We will not get it perfect, but we need that ability for industry to share with us the fact that these attacks and exploits are going on. But if we cannot stop them, we cannot help.

There are five areas that I focused on with our folks, with the folks at U.S. Cyber Command.

First, we have to build and train cyber forces. And these are things that Bob Kehler and I are arm in arm on. These are the key things that we have got to do.

Second, we have to have a defensible architecture. You mentioned the 15,000 enclaves, and the reality is our integrated architecture, the way that we have set them up, if went to the way Google, Yahoo, and others are doing it in the Defense Department, we would have a more defensible architecture. And that is the way we are pushing, and the services are helping us get there.

I think we have to partner with DHS and FBI. The reason that I bring DHS into this is that I believe we want them working with the rest of Government to help set up the rest of Government networks and work with that. We do not want to take the people that I have and push them over here. I think we want the people that we have looking outside, and I think that goes to Senator McCain's comments. We are the offensive force. We are the ones that are going to protect the Nation. We need to see what is going on and be prepared to do that. We can give and work with DHS and provide capabilities and technical expertise, and that is growing.

Finally, I would add in FBI. They have some tremendous capabilities. They have the law enforcement arm.

And when you put all three of us together, I think our country knows that what we are doing is transparent and we are doing the right thing. And in doing that, you have brought all three players to the table.

I see command and control and partnership as key especially with our allies, and I would put the allies on the table because this is going to be huge for our future.

And the concept for operating in cyberspace we have mentioned earlier.

So it is an honor and privilege to represent the soldiers, sailors, airmen, marines, and civilians of U.S. Cyber Command here today. I thank you for the opportunity to discuss our many accomplishments and progress in building capabilities to perform our mission in the future.

I would ask that my statement for the record be included on the record.

And that is all I have, Chairman.

[The prepared statement of General Alexander follows:]

Chairman LEVIN. Thank you so much, General. Your statement will be made part of the record.

We will start with a 7-minute first round.

General Kehler, first, do you support the fiscal year 2013 budget request?

General KEHLER. Yes, sir, I do.

Chairman LEVIN. General Kehler, you made reference to an effective nuclear command and control network that needs improvement, I believe, in your opening statement. Are those efforts underway to modernize that command and control network? Can you describe those efforts a little bit?

General KEHLER. Yes, sir, I can. Of course, as you know, the nuclear command and control system is composed of many, many parts. There are parts of the nuclear command and control system that are not survivable. However, inherent in the nuclear command and control system is a thin line that ultimately would be survivable under any conditions so that we could always ensure that the President of the United States is connected to the nuclear forces.

Investments are underway in those critical capabilities, the capabilities that are part of the space architecture layer, of course, advanced EHF satellites. The first one is on orbit. The second one will go to orbit in the next year or so. I do not have the exact date. That will be the satellite-based survivable part of our thin line network as we go forward.

We have some issues with terminals and terminals lagging the deployment of the satellites. That means we are going to have to use older terminals. We will not get the full capability about of the satellites at first. We are working that problem.

We have some issues to make sure that our bomber connectivity is maintained. The Air Force program supports that, and so I am comfortable that we are going forward there to maintain the connectivity at the force end of this.

We are also upgrading some of our other components to the network, ground-based parts of the network, et cetera.

So I will always be a little uncomfortable about the network. I will tell you that I think there is more to be done. We are working that inside the Department for future budget requests. In fact, we are undertaking a fairly substantial review at this point in time about the nuclear command and control system and how it does or does not support other issues as well.

Chairman LEVIN. Thank you, General.

The 2010 nuclear posture review called out for studying additional reductions in nuclear weapons. Do you think it is possible to further reduce our nuclear weapons beyond the New START levels?

General KEHLER. Mr. Chairman, I think there are opportunities to reduce further, but I think that there are factors that bear on that ultimate outcome. And rather than get into those, which I do not think would be appropriate, I would just simply say I do think there are opportunities here, but recognizing that there are some factors that bear on this.

I would also mention it is never our view that we start with numbers. We start with an assessment of the situation we find ourselves in, the strategy, our objectives, et cetera, and ultimately then you get to numbers.

Chairman LEVIN. Thank you.

General Alexander, are you advocating for any additional legal authorities that are not included in the cybersecurity legislation that was proposed by the administration to Congress or that is included in the Lieberman-Collins bill?

General ALEXANDER. No, Chairman.

Chairman LEVIN. The industrial espionage campaign I noted in my opening statement, and you made reference to it in your statement, particularly China's aggressive and relentless industrial espionage campaign through cyberspace.

I wonder. Can you us some examples in open session of the technologies that have been stolen through penetration of major DOD contractors and perhaps the Department itself, and do you know whether or not in fact we have raised this issue, particularly Vice President Biden, with the Chinese?

General ALEXANDER. Senator, I am not aware on the last, what Vice President Biden has shared with the Chinese for that discussion.

But we are seeing a great deal of DOD-related equipment stolen by the Chinese. I cannot go into the specifics here, but we do see that from defense industrial base companies throughout.

There are some very public ones, though, that give you a good idea of what is going on. The most recent one, I think, was the RSA exploits. RSA creates the two-factor authentication for things like PayPal. So when you get on and order something and pay for it over the network, the authentication is done by encryption systems that RSA creates. The exploiters took many of those certifications and underlying software which makes it almost impossible to ensure that what you are certifying or what someone else is certifying is in fact correct.

Now, RSA acted quickly and is replacing all those certificates and has done that in priority order for the Defense Department and others.

But when you think about it, the ability to do it against a company like RSA is such a high-order capability, RSA being one of the best, that if they can do it against RSA, that makes most of the other companies vulnerable.

Chairman LEVIN. Well, we took some action in the counterfeiting area in our defense authorization bill to try to stop that type of theft, particularly again by the Chinese when it came to the supply of parts for weapons systems. I think it will be important for you to talk to Vice President Biden or his office so that you can see what steps were taken to inform the Chinese of our position on this.

And we have now got to find ways—and I think you are the perfect person to be a spokesman for this—to stop their theft of other kinds of intellectual property through the use of cyber.

I wonder if you could give us some examples or give us some options. I think Senator McCain also made reference to this. What are the options for us in terms of action for them or anyone else who is stealing our information or our intellectual property to pay a price for this?

General ALEXANDER. Well, I suppose using the rest of STRATCOM would be out, Chairman.

I think the first thing that strikes my mind—and I want to be clear on this because the most important thing that we can do right now is make it more difficult for the Chinese to do what they are doing. The analogy that I put on the table is we have all our money in our banks, but our banks have the money out on tables in New York City at the park. And we are losing the money, and we are wondering why. Nobody is protecting it or it is not well protected. Our intellectual property is not well protected and we could do better protecting it. So step one is take those steps to do that.

I do think what the Department is doing—you asked for authorities that would need legislation. I think those are in the legislation. And what the Department is doing with the authorities we already have is maturing the standing rules of engagement that would allow us to stop some of these exploits as they are going on. I think we can do that with minimal risk, and I think those are some of the things that we can do. Stop them in progress.

As an example, we saw an adversary trying to take about 3 gigabytes, a lot of information, from one of our defense contractors. We saw that in foreign space. And the issue was now we had to work in human space to reach out to them to say they are trying to steal something. You have got to stop it. There has got to be a better way to do that because that is almost like going at network speed now trying to send a regular mail letter to them that you are being attacked. And so we have got to bring this up into the network age to get these responses out.

So I would advocate—and I think the way we are going is—to, one, build our defense and, two, have options that would stop it.

Beyond that, I think the President and the Secretary need options that would take it to the next step. These are not options that we would take, but these are options that we would propose to the administration. If they exceed certain limits, I think it is our responsibility jointly and with the COCOM's to say here are the options you can now take to stop these acts. And depending on the severity of the act, here is what we would propose to be done.

So I think our job would be to defend and protect and to stop some of these attacks, analogous to the missiles coming in, and give the administration options of what they could do to take it to the next step if they choose. Those include cyber and other options that are available. And I think the White House has put that forward in their cybersecurity thoughts.

Chairman LEVIN. Thank you.

Senator McCain.

Senator MCCAIN. I want to thank the witnesses.

I would ask General Alexander. Do you agree that Secretary Panetta and the FBI have said that cyberattacks may soon be the number one threats to the United States?

General ALEXANDER. Absolutely, Senator.

Senator MCCAIN. And would you agree that the major threats to our national security come from outside the United States specifically, obviously from unclassified information, from China?

General ALEXANDER. Absolutely.

Senator MCCAIN. Absolutely. So then what is the logic in providing the overall authority to the Department of Homeland Security? Anyone who has been through an airport, as I do regularly, as most of us do, have no confidence in the technological capabilities of the Department of Homeland Security. In fact, as an example nothing has changed as far as airport security is concerned since probably September 12th, 2011. So the major threat comes from overseas. What would be the logic then in making the lead organization the Department of Homeland Security?

General ALEXANDER. Senator, I think the issue—if I could, I want to break this out into three areas to make sure my response is—

Senator MCCAIN. And make it brief please. I have additional questions.

General ALEXANDER. Yes, sir.

I see three major things. We want DHS to take the lead on resilience in working with civilian agencies and critical infrastructure. We want DOD to take the lead on defending the Nation under cyberattack, FBI under law enforcement and intelligence. And I think all three of us need to work together as a joint team to move this forward. If we do not work as a team, then the Nation suffers. So inside the United States, that is where I think DHS has the lead. They do not in terms of the foreign and the things coming in. That is where you would want us to have the lead.

Senator MCCAIN. How many people are under your command?

General ALEXANDER. In Cyber Command, counting our service components, a little under 13,000.

Senator MCCAIN. So we now have 13,000 and Cyber Command was recently formed up. So now we need other agencies. Why should the responsibility not lie with Cyber Command?

General ALEXANDER. Senator, I do think the responsibility for defending the Nation against attack lies within Cyber Command out. I think the lead for lead for working with critical infrastructure and helping them defend and prepare their networks should lie with DHS.

Senator MCCAIN. That is a curious logic, General, in fact, most curious.

So really all we formed up Cyber Command for was to worry about external threats. Is that what you are saying? So the Department of Homeland Security should take the lead for anything that happens in the United States from outside, but you are still there with your 13,000 people?

General ALEXANDER. Not quite that way, Senator. Probably I am not clear enough on this. In terms of DHS's roles and responsibility is working with critical infrastructure and other Government agencies on developing the standards and the protocols of how they build their networks and to be the public interface. I think that is the role that we want them to do. And their people go out and reach out with critical infrastructure and make sure those Government systems are adequately developed.

If they are attacked, no matter where that comes from, now I think the President has options of what he can do. We are one of those sets of options, and if chosen, we are prepared to do that.

More importantly, where those people really come in is in our offensive capabilities. You asked that earlier. So the offensive capabilities would be to support the other combatant commands and their plans and capabilities.

Now, the bulk of our——

Senator MCCAIN. So your job is to support other commands with their offensive capability. You know something, General? One of the conclusions of the 9/11 Commission was there is too much stovepiping in our intelligence community. You are just describing stovepiping to me at its ultimate.

General ALEXANDER. Well, that is not the intent.

If I could go one point further, the bulk of our forces are folks that operate and defend the DOD networks. That is where we are today. The bulk of them are operating and defending our networks. So if you think about what the Army, Navy, and Air Force do in operating and defending the networks, that is the first mission that U.S. Cyber Command was given. We are developing the second parts of that.

But I would point out, when you say stovepipe, Senator, I do not agree with that because this is an integrated network. It is one network trying to work everything together. So it is just the opposite of a stovepipe.

Senator MCCAIN. Well, it is interesting that Michael McConnell at George Washington University, former Director of National Intelligence, said current U.S. cyber defenses are weak and the bills on Capitol Hill are insufficient. So, obviously, the former Director of National Intelligence has a significant disagreement with your assessment.

So according to a recent article in the Washington Post, the White House blocked draft legislation that would have given NSA or any Government entity the authority to monitor private sector networks for computer viruses and to operate active defenses to block them. The NSA supported the authority but the White House did not. According to an administration official, blocking of the draft caused some consternation because NSA wanted to get that authority.

There are some who propose that NSA should be able to detect but not read the cyberattack information. Do you agree or disagree with that?

General ALEXANDER. I disagree. I think the approach that we have put on the table is the appropriate one which is we give that to industry. They can look at that and when they see that, tell us. I think that is the first right step, Senator. I think if we go too far, it sends the wrong message, and I think we can take this journey and learn as we go on it.

Senator MCCAIN. So you believe that DOD—General Cartwright, the former Vice Chairman of the Joint Chiefs of Staff, said DOD is spending 90 percent of its time playing defense against cyberattacks and 10 percent playing offense and that the Department should invert this defense/offense ratio to signify that a cyberattack on the United States will have negative consequences.

And your answer, as I understand it, is, well, we will act in some way or fashion. Perhaps you can be a little more specific how we can gain the offense here.

General ALEXANDER. I actually agree with his statements, and I would like to characterize it in my words, if I could, Senator. More than 90 percent of our force was developed—all of our force in cyber, as we started, was on the defense and operate. We did not have offensive capability. And so what we are looking at now is how do we grow that capability. So if you think about what we have within our fleets, air wings, and brigades is the operate and defend capabilities. The offensive capability primarily lies in the exploitation capabilities of NSA and others. We are developing those.

I agree that we need to develop those more and faster, and we are working on that with the services and that is part of our growth plan.

I think, in terms of this, Senator, I do not want to give you the impression that I do not believe we should defend the United States. I do. But I do think we can do that in a way that works with industry without having us in the middle of the network. They share the information with us, and I think that is the right first step to take.

Senator MCCAIN. And industry, according to industry, does not need additional regulations. They need the ability to share information which is our proposal rather than additional new Government regulation implemented by probably the most inefficient bureaucracy that I have ever encountered in my number of years here as a Member of Congress. The Department of Homeland Security wasted $887 million on a virtual fence on the Arizona-Mexico border, that has made not a single technological advance as far as airport security is concerned to ease passengers' transit from one place to another, and has shown an incredible ability to illustrate inefficiency at its best.

I thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator McCain.

Senator Lieberman.

Senator LIEBERMAN. Thanks, Mr. Chairman, and thanks to both of you.

Obviously, my friend from Arizona and I have a disagreement here. The first thing I want to do very briefly is come to the defense of the Department of Homeland Security. The fact is that we have not had a major terrorist attack on the United States since September 11, and you have to give the leadership, bipartisan over two administrations, and the thousands of people who work at DHS some credit for that.

Second, in terms of the stovepiping, I think a better analogy here—and it is not a perfect one—is to compare the relationship between the CIA and the FBI to the relationship between Cyber

Command and NSA and DHS. CIA has authority outside of the United States of America. The FBI has authorities—I am speaking about terrorism, for instance, or threats to the Nation. FBI has authority within the country. The problem before September 11 is that they were stovepiped. They were not cooperating enough. In the same way, NSA's Cyber Command, as you have said, has the responsibility to protect America—it is a jewel. It is a national treasure—from cyberattack, along with many other responsibilities that you have. DHS has a domestic responsibility, a preventive responsibility. In that sense, it is a little different and less expansive than FBI in the other case.

The interesting thing that you have testified to and I think Senator McCain was not hearing is that you are building exactly the kind of cooperative relationship between NSA Cyber Command, DHS, and the FBI that did not exist before September 11. And the fact is Senator McCain and I introduced an amendment to the National Defense Authorization Act last December that codifies in law the working agreement between NSA and DHS.

Incidentally, I will just say this for the record. I have talked to Admiral McConnell, a former DNI. I have heard him speak in a public setting. He thinks both bills are not strong enough, but if you ask him do you prefer the Cyber Security Act of 2012, which Senator Collins, Feinstein, Rockefeller, and I have put in, or the SECURE IT, which some of my colleagues have put in, he could not be clear. SECURE IT does do it because it does not provide for defensive preparation by the private sector.

Look, I know the private sector is lobbying against this. I think there is a terrible trap here. This is not just a question of regulation of business. This is a protection of our homeland. You have told us in response to Senator McCain's question—General Dempsey, Secretary Panetta, Director Mueller—cyberattack is the main area of vulnerability we have today. Shame on us if we look at this as business regulation. This is homeland security. And we have got to get together before too long and make this happen.

I want to come to the particular difference between the two bills. There are two critical things that have to be done here in my opinion. There are many important things. One is an information sharing authorization section. The other is protection of the most critical cyber infrastructure which is owned by the private sector, 90 percent of it, finance, transportation, electricity, water, all of which is vulnerable to attack by an enemy.

Both bills have information sharing. Only the bill that Senator Collins and I have introduced has a provision for the Department of Homeland Security to work with the private sector to require the most critical covered infrastructure, not every business, to take certain actions to defend their network, to defend our country.

General Alexander, I believe I heard you say—I just want to have you confirm it—that you believe we need both of those authorities in Government, that is, information sharing and a system for protecting and better defending privately owned, covered critical infrastructure. Is that right?

General ALEXANDER. Senator, that is correct. As you have stated, that is the hard part is determining. So how do you do that in such a way as not to burden industry? But I do think we have to set up some standards. I am not sure that we—you know, we use what we call the gold standard. And the gold standard was one that we thought provided our networks the best defensible posture. And we give that out free. We put it on the nsa.gov as here is a set of standards. I think as we work with industry, the issue is how do you make sure that they are as defensible as possible without being over-burdensome. And so I do think that we have to set that up. It is like roads, like cars.

Senator LIEBERMAN. Exactly. This is not regulation actually. These are standards for what we are going to ask them to do to defend our country. And they are then going to figure out how to do it.

Incidentally, you know, business is understandably worried about their bottom line. We have got to be worried about the security of the American people.

Incidentally, I take it from what you said earlier that the fear of a cyberattack against the United States—I mean a major cyberattack—is not theoretical but real in your mind, General Alexander.

General ALEXANDER. That is correct, Senator.

Senator LIEBERMAN. And it literally could happen any day. I am not predicting that it will. But right now our privately owned cyberspace infrastructure, as compared and distinguished from DOD's, is vulnerable to attack. Is that correct?

General ALEXANDER. That is correct, Senator. In fact, if I could add, it is my opinion that every day the probability of an attack increases as more tools and capabilities are out on the Internet.

Senator LIEBERMAN. Right. It is very important for people to hear that.

I want to relate the requirement on the most critical covered infrastructure to take some defensive action to your description that I thought was excellent about what you mean when you say you want to see an cyberattack coming. You have made very clear that you do not want NSA into our private cyber systems, but you need to have the private cyber systems be able to tell you when an enemy attack is coming. Right?

General ALEXANDER. That is correct.

Senator LIEBERMAN. So you can act. And to me that is probably the most significant gain that we will have from the Department of Homeland Security, informed by you, setting these standards for defense for the privately owned cyberspace. Look, I hear so many stories about critical infrastructure operating systems using defensive systems that are 15 years old without even basic detection capabilities. I think one of the most important things that is going to happen, as a result of the system we are talking about, is that the most critical infrastructure—not every business at home, but the most critical infrastructure—will have to develop within itself or hire some of the private companies that do this the defensive systems that will let them know, which a lot of them do not now, when they are being attacked so they can immediately get to you so you can spring into action to essentially counter-attack. Is that correct?

General ALEXANDER. That is correct. And under what conditions is what the administration and the Department is looking at on the rules of engagement. So when we actually do that, those will become the rules of engagement that we are working on.

Senator LIEBERMAN. Let me just ask finally is your relationship under the memorandum that we codified into law with the Department of Homeland Security working well as far as you are concerned.

General ALEXANDER. It is. It is growing. And I think the key thing Secretary Napolitano is wonderful to work with. She came out to NSA and Cyber Command and had a chance to sit down with all of us. Absolutely her heart is in the right direction. She understands what we bring to the table. She leverages that not only in the cyber mission but across the board. And I think we are making the correct strides.

When you add FBI's tremendous technical capabilities in there, that is the team that I think the Government wants and needs in place. You know, the reality is we can put all of our manpower internal and it will not solve the problem. We have to work together as a team. I do believe that is the best way to approach it. So——

Senator LIEBERMAN. Sorry.

General ALEXANDER. So I was going to say, to answer your response, DHS has been good to work with. They are growing their capabilities. It will take time. We provide a lot of assistance to that, and we think that is a good relationship.

Senator LIEBERMAN. And that is exactly what they tell me: good relationship and they are benefitting enormously from your extraordinary expertise. Thanks, General.

Thanks, Mr. Chairman.

General KEHLER. Senator Lieberman, could I add a comment?

Chairman LEVIN. If you make it brief.

General KEHLER. It will be very brief.

This is really about balanced responsibilities. When you look at balancing the responsibilities between the military, the intelligence community, law enforcement, and the Department of Homeland Security, if we were not talking about cyber, we know how to do that. We understand what that balance looks like. We understand that when DHS needs military support, we have what we call defense support of civil authorities. We have ways that we can provide support to them.

The question is what happens when you add cyberspace to this mixture, and that is the balance that we are trying to make sure that we are striking. I think that is an important point for us as we go forward. The bottom line here is all of us working together to improve the protection of our Nation and the national security.

The second point that I would make quickly is there are basically three things we are going to have to do here. One is protect ourselves better related to cyberspace for the very reasons that you mentioned. The second is we have got to become more resilient, recognizing that we are not going to be perfect at protection or defense. We have got to be more resilient, particularly on the military side. And then lastly, we have got to do better at an offensive capability and balance that in a better fashion as we go forward.

Chairman LEVIN. Thank you, Senator Lieberman.

Senator Inhofe.

Senator INHOFE. Thank you, Mr. Chairman.

The first question I am going to ask I already know the answer, but I am going to have to ask it just to get it in the record.

In yesterday's Wall Street Journal, they talked about President Obama's meeting with Russian President Medvedev yesterday, Monday, when President Obama said—and I assume he said this without knowing that the mic was on, but this needs to be in the record. And I would ask the reflect this accurately. Quote: On all these issues, but particularly missile defense, this—this can be solved, but it is important for him, incoming Russian President Vladimir Putin, to give me space. This is my last election. After my election, I have more flexibility. Unquote.

So the question is do either one of you want to comment? [No response.]

I did not think so.

The second thing that I would like to mention is that—General Alexander, first of all, I thank you for making the trip that you made out. Just real briefly, kind of tell me what you found out during your visit to Tulsa University.

General ALEXANDER. Thank you, Senator. First, there are two things.

I am really impressed with the way the American people, especially in Tulsa, have come together to help fund that university and the young folks that go there. And from my perspective, one of the key things—and I should have thought about this earlier—that Tulsa University is doing is in the information assurance area, coming up with better ways to defend networks. And when you think about that, that is exactly what we are talking about on the resilience side. So when you look at what those young people do, they find problems in networks. They showed us some in the SCADA system and others that if we now made some slight changes, I think those changes and upgrades in the security of those networks would make them more secure.

So what I found was tremendous young people doing great things, some of whom we have hired, and we continue to hire from Tulsa and other universities throughout the country that are doing programs like that in the information assurance area. So thank you.

Senator INHOFE. And I thank you for going out. One of the things that we do have that you probably witnessed was the community support behind the program, behind the university. So anyway, it is a good program.

General Kehler, back during the time that we were considering the bill a year ago, we were talking about the fact that President Obama was weighing options for sharp new cuts in our nuclear arsenal unilaterally. And then, of course, that was an agreement with Russia to bring it down to the 1,550. I guess it was a month ago, it was reported that President Obama is weighing the options of sharp new cuts to our nuclear arsenal unilaterally, potentially up to—and these are the figures they used—80 percent proposing three plans that could limit the number as low as 300.

Now, it was in 2008—I always remember and I carry this with me—Secretary Gates stated as long as others have nuclear weapons, we must maintain some level of these weapons ourselves to deter potential adversaries and to reassure over 2 dozen—that is about 30, as I understand it—allies and partners who rely on our nuclear umbrella for their security, making it unnecessary for them to develop their own.

Now, I would like to ask what kind of implications this would come up with in terms of our allies, those 30 other countries that are depending upon our umbrella, if we were to voluntarily bring it down 80 percent.

General KEHLER. Sir, I would make a couple of points.

The first thing I would say is, as I said earlier, we do not start with numbers. We have been starting with strategy objectives, national security objectives, et cetera.

The study that you referred to is still ongoing. No conclusions have been reached yet, and so it is not appropriate for me to comment on the study. STRATCOM has been a full participant in the study, and I believe that, as I said earlier, there are opportunities here for additional reductions. But that is——

Senator INHOFE. Unilateral reductions.

General KEHLER. Well, sir, all along here and going all the way back to the nuclear posture review, I think the viewpoint has been that it is best to do this with Russia. The Russian and the U.S. arsenals still really drive this conversation, and so doing this with Russia is certainly the preferred way forward. And I think that the need to continue to deter and assure allies remains.

Senator INHOFE. Well, okay. The point I am getting to, though, is the key word is “unilateral,” and that is what concerns me.

General KEHLER. Yes, sir.

Senator INHOFE. Let me, just real quickly, cover just a couple of other things here.

This, General Kehler, was the triad—I think it was about 2004 or 2005—showing the cliff. You are somewhat familiar with that. Now, I am wondering if we could get this updated. First of all, during the consideration of the New START, the President said: I intend to modernize or replace the triad strategic nuclear delivery system, a heavy bomber, air launch cruise missiles, and ICBM, and nuclear powered ballistic missile submarine and SLBM, and maintain the United States? rocket motor industrial base. He goes on and elaborates on that.

Now, this statement was made after this chart. Do you have an updated chart on this that would reflect what is happening today?

General KEHLER. Sir, may I take that for the record and get back to you?

Senator INHOFE. Yes, you certainly may. That is very reasonable.

[The information follows:]

[COMMITTEE INSERT]

eneral Kehler: I am happy to do that.

Senator INHOFE. Then the last thing on that is something that no one ever talks about but I have always been concerned, and that is relating to the tactical nuclear weapons. Several of us on this side of the aisle and on the other side of the aisle made an effort to include tactical nuclear weapons at the time that we were looking at the New START program. And as it is right now, it is about a 10 to 1 advantage of Russia over ourselves. Do you agree or disagree with me that that should be a part of the plan?

General KEHLER. I agree that it should be a part of the plan. Yes, sir.

Senator INHOFE. All right. Thank you very much, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Inhofe.

Senator Nelson.

Senator NELSON. Thank you, Mr. Chairman.

And thanks to both of you for your service and for your kind remarks this morning. I appreciate that very much.

General Kehler and General Alexander, the comments today and all the discussion for some period of time has indicated the growing threat of cyber warfare threat to the United States' national security. As we engage in this discussion, there is an ongoing restructuring of STRATCOM's headquarters with a new headquarters at Offutt.

General Kehler, can you give us some indication why an aging facility would not be an appropriate facility as we take on new responsibilities but particularly as it relates to the high-tech cyber situation?

And General Alexander, if you had some thoughts about that, it would be helpful too. Thank you.

General KEHLER. Sir, the activities that go on at STRATCOM are unique activities. We perform those activities, particularly the command and control that we have for our strategic forces, the planning that we do for our strategic forces, the intelligence support that is required behind our continuing need for strategic-level deterrence and being able to command and control forces under high stress. All of those really come together at STRATCOM headquarters.

The demand that today's systems place on that headquarters building have far outpaced the ability of the building to keep up. Not only do we have vulnerabilities because of the cyber concerns that we have expressed earlier, but we have physical plant vulnerabilities there. You are well aware of some of the failures that we have had, catastrophic failures, in the building systems themselves that have threatened to take that one-of-a-kind location and really make it inoperable for months. We barely averted that kind of a catastrophe a year ago in December with a flood, of all things, in the basement, a burst water line.

And so as we looked at ways forward, given the unique nature of what we do, given the one-of-a-kind responsibilities that are performed there and given the continued importance of all of that in our deterrence posture, the conclusion that the engineers reached was that you could not modify the building, that basically what you needed to do was go and build a new command and control facility that houses all of the activities that we are going to need to perform.

That remains my assessment today, that we need to get moving on this. I think that it is proceeding well. I believe that we are headed toward contract award. I know the Corps of Engineers has responsibility in this regard, and things seem to be moving forward, at least everything that I can be aware of. And much of this, of course, needs to be in the realm of the Corps and others.

So from my perspective, Senator, the bottom line is the recognition that we do something unique there, that it is not about a brick and mortar building. It is about what goes on there in the computer systems and the need for support systems, information technology, and the supporting networks that put all of that together so that we are prepared to continue to perform this deterrence mission as far into the future as we can see.

Senator NELSON. Thank you.

As you know, when it comes to the CMR replacement facility, NNSA has deferred for 5 years the construction of the Chemistry, Metallurgy, and Radiological, or CMR, replacement facility. Is this, the CMR replacement facility, a concern for you in not only meeting our responsibilities and obligations and commitments on the New START treaty but just in general keeping our arsenal current?

General KEHLER. Senator, it is a concern for me. I think of all of the items in the 2013 budget, those items that would be associated with STRATCOM's portfolio of mission responsibilities, fare generally pretty well. There were some delays and programmatic adjustments and other things that were made. I think we can manage risk across all of that.

When I look specifically at the weapons complex, the ability of the complex to provide us the weapons that we need that have the appropriate life extensions provided, that give us the flexibility to manage the hedge and allows us to look at potential reductions, as we go to the future, in the stockpile, I think the thing that concerns me the most is our continued investment in the weapons complex. And so the issue with CMRR does concern me. I understand the 2013 budget does provide for us to get moving in a number of areas.

The Secretary of Energy and the Secretary of Defense sent a letter to the Congress that reminded them that we are not ready yet to lay out what happens in 2014 and beyond. Until we are ready to lay all of that out, I remain concerned.

Senator NELSON. Well, it could be appropriate to at least start the process as in the case of the STRATCOM headquarters which is going to be a phased-in funding over several years. At least a start could be made on CMR in a similar fashion. Otherwise, it looks like we have just put together baling wire and maybe a duct tape structure to get us through 2013 budget-wise.

General KEHLER. Senator, this is ultimately a do-out from the Departments of Energy and Defense, and we owe you the alternatives. I do not have with me today, because we do not have yet, a set of viable alternatives that we can come and present. I do agree, though, with the main thrust here and that is I see no alternative, as we look to the future, aside from modernizing the complex.

Regardless of what happens, we have a fairly extensive backlog of weapons awaiting dismantlement that require the same kind of a modern complex to dismantle. So I think from both sides of this equation, we need a modern weapons industrial complex. It is highly unique and it is very specialized. We need that kind of a complex so that we have a safe, secure, and effective deterrent.

Senator NELSON. It is hard to draw an analogy other than to say that trying to put together something on a stop- gap basis might get us through 2013 but does not position us for what we might do years beyond and particularly with an aging stockpile.

General KEHLER. Senator, we owe you some answers, and the study to produce those is underway.

Senator NELSON. Thank you.

General Alexander, as you relate to the responsibilities with cyber, I think you made it very clear that there is a role for the DOD. There is a role for Homeland Security. There is a role for our law enforcement agencies, and continuing to find ways to work together is a reduction of stovepiping that has been so predominant in the past.

Are you comfortable that the agencies that are all trying to work together understand the important need not to stovepipe and to break down even with some comparable authorities that will go to different agencies, but to continue to work together on this important threat to our country and to our business, which is also a threat to our country?

General ALEXANDER. Senator, I do.

Senator NELSON. Thank you. Thank you, gentlemen.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator Nelson.

Senator Brown.

Senator BROWN. Thank you, Mr. Chairman.

General Kehler, I was wondering do you consider the Global Strike Command pretty valuable. Let me restate that question. I am sorry.

Would you consider the air operations groups currently supporting the Global Strike Command a valuable resource?

General KEHLER. Senator, yes, we sure do.

Senator BROWN. Are they irreplaceable? Are they such an integral part of what you are doing that if you did not have them, we would be in trouble?

General KEHLER. The entire force that Global Strike Command brings to STRATCOM—in fact, that is one of Air Force components, one of our major components as a matter of fact. They bring us the entire dual-capable bomber force, the B–52s and the B–2s. They also bring us the entire ICBM force. They bring us an air operations center that allows us to manage all of our air activities in STRATCOM. And so what Global Strike brings—and all of its subordinates are all very valuable to us.

Senator BROWN. And that actually provides real-world, time-sensitive planning support as well. Correct?

General KEHLER. Yes, sir.

Senator BROWN. When you are answering those questions like that, that is why I am a little concerned with the Otis Air National Guard Base. I was there a couple of months ago, and they have a great mission and their air operations group supports STRATCOM's Global Strike Command by providing exactly what you have indicated, the irreplaceable, real-time, sensitive support. And yet, I have heard that the Air Force wants to break up this very valuable, irreplaceable unit to save money. And I was wondering if, number one, you were aware of or were given the opportunity to comment on that proposal affecting that group and Otis in particular.

General KEHLER. Senator, if I could take that for the record, I would appreciate that. I do not know enough about the details.

Senator BROWN. Okay, that would be helpful because I agree with you.

[The information referred to follows:]

[COMMITTEE INSERT]

Senator BROWN. I agree with everything you just said in your opening response to my questions, that it is irreplaceable. It is valuable, and I know what these folks do there. And especially being on the eastern seaboard of the United States and covering all of the eastern United States in some respects, I mean the Air Guard in particular and Army Guard as well and Reserves—they give you great value for the dollar. And I am deeply concerned that we are cutting off our nose to spite our faces. It is kind of like the Air Force is saying, okay, I am going to keep all my toys here, and by the way, the Guard and Reserves—we are going to take away what you have. I have not been yet convinced that these cuts represent either an acceptable level of risk or an efficient use of the money. So I would ask—and I will get you the very specifics questions for the record. And I appreciate that.

I know we are talking about cybersecurity. I know there are many proposals. We have one in Government Regs and the administration. The military is working on a whole host of things. How are the rules of engagement actually working or being implemented or coming along with regard to the Cyber Command operation?

General ALEXANDER. Senator, right now we are upgrading——

Senator BROWN. I meant that to you, General Alexander. I am sorry.

General ALEXANDER. Right now we are updating, if you will. The rules of engagement that the chairman has put out were dated in 2005. Given where we are today, what the Joint Staff has taken on is to update those. Right now all our measures are internal to our networks, what DOD is authorized to do. What we are looking at within DOD and then within the interagency what are the next steps that we should have and how do we take those steps. I think over the next month or 2, the Joint Staff will complete those standing rules of engagement and then move those to the interagency and share those.

Senator BROWN. What role do you see or what segments of the private sector should fall into DOD's responsibility, if any?

General ALEXANDER. This is where the discussion comes in. First——

Senator BROWN. And let me just extend on that. If attacked, what entities would be considered an extension of U.S. Government facilities?

General ALEXANDER. Well, I think those are decisions that you in the bills and the administration would make on when we actually implement response options or response options to defend against an attack. That is the first step.

So let me start with technically what we are doing. I think the first part of that, Senator, is to have the information sharing, to know that an attack is going on. We discussed that a little bit previously. That is the ability for industry to tell us that something is happening and that either FBI, if it is domestic, DHS, or if it is foreign, that FBI and Cyber Command and NSA would respond to.

The issue and I think what we are going to walk our way through candidly is we have got to start someplace. And I think putting out where we are on the information sharing and having industry take the lead with DHS on providing us the insights of what is going on is the first right step. I think that is the best step that we can take.

More importantly, I think we need to take that step. What we cannot do is wait. And I think your question and where you are going on this is absolutely right. We have got to take measures now, and I think those are absolutely important because my concern and the statements that go to that is that if somebody is attacked, the way we find out about it today is after the fact. You cannot stop it then. Now you are in the forensics mode. And so I think what everybody agrees is so we have got to get to a point where industry can tell us when something is going on so that we can help prevent it.

And then the options come up to what industry has included in that. And those are parts of the bills that I know that you are all considering.

Senator BROWN. And that is great, but I tell you what. We do not have all the answers. I can tell you that firsthand. And what I am concerned about is that we create a bill that has so much red tape and so much overlap and duplication that you cannot get out of your own way. So I would ask for your recommendations and guidance as well to be part of the process and let us know what your thoughts are and where you feel the weaknesses or strengths lie so we can expand or detract from that.

And I am deeply concerned, and I think you are right. I know you are right in the fact that we are always reacting instead of being proactive, and when that attack happens, we find out about it after, after our technology and intellectual property and military secrets and plans are stolen. And that deeply concerns me.

I was wondering as the technology continues to advance, potential cyberattacks are capable, as you know and I think have referenced, and executed at increasing speeds. Do you have enough leg room from the authorization standpoint to act at the earliest possible opportunity to defeat a cyberattack before it is launched? Do you have enough flexibility do you think?

General ALEXANDER. Those are some of the issues that are being considered in the rules of engagement. And so I will not know until we are complete with that. We are pushing for what we think we need, and I think what the Chairman and the Joint Staff and then OSD will do is say, okay, what makes sense.

Being extremely candid on this, it really comes down to so what are those actions that make the sense that we could do defensively, analogous to the missile shoot-down. And I think there are some there that we are getting agreement on, yup, it makes sense to stop that attack from going. But if you were to go after a computer in foreign space or some other thing, that might be a response option that would now take, I think, the President and the Secretary to step in and start making decisions versus us taking that on. And

I think that is probably where we will end up. And that makes a lot of sense from my perspective.

Senator BROWN. Well, first of all, thank you very much, both of you. This is an issue that deeply concerns me and many other members of the committee. I will be submitting some questions for the record or maybe we can speak offline. I do not want you to have to reinvent the wheel, just some certain areas that I think I need a little bit more understanding of. Thank you very much.

Chairman LEVIN. Thank you, Senator Brown.

Senator Hagan.

Senator HAGAN. Thank you, Mr. Chairman.

And I thank both of you for your testimony today and certainly for your service to our country. Thank you.

General Alexander, the administration believes that it is crucial for critical infrastructure companies to carefully diagnose their cyber vulnerabilities and the risk posed to the American people should these vulnerabilities be exploited and to take steps to eliminate these vulnerabilities. The administration has proposed legislation to ensure that industry stands up to these responsibilities as a matter of national security. The administration is also seeking to extend the signature-based defense that the NSA and that U.S. Cyber Command have developed for DOD's critical infrastructure.

Since the administration is seeking to implement both approaches, the implication is that neither one alone is seen as sufficient to meet the threat. Others, however, take the position that information sharing, in conjunction with the National Security Agency's defensive solution, would be enough, that it is not necessary to require critical infrastructure companies to build up their own defenses.

Do you believe that NSA's signature-based defense deployed recently in the defense industrial base pilot program can defend our Nation's critical infrastructure against nation state cyberthreats, or do you believe that the critical infrastructure companies also need to close their vulnerabilities?

General ALEXANDER. Senator, first, I think it is the latter. We need both. But I would like to take it one step further because I do not think what we are talking about is having NSA deploy capabilities out there. Rather, what we are talking about is NSA providing technical capability to others to run, nor we do not want run stuff within industry. So I want to make that clear. It is not us putting stuff out there for us to operate. What we are really saying is industry has a bunch of signatures that can detect foreign actors that are coming against them. Government has some of those. NSA, DHS, and FBI, all of us need to work together to provide the best set of signatures to protect that critical infrastructure. Industry can actually operate that and tell us when that occurs.

I also think that you need to set a set of standards for how those systems are operated to give you the best and I will call that—and General Kehler mentioned it and it is in there—resilience. We need the resilience in those networks to ensure that they can operate and be defensible while we are trying to defend the country outside.

Does that make sense?

Senator HAGAN. Yes.

Just last Friday—and I read about it yesterday—Microsoft was accompanied by U.S. marshals and they raided office buildings in Pennsylvania and in Illinois to disrupt a group of computers, a botnet, that was harvesting bank accounts, passwords, and other personal information from millions of computers. And Microsoft's actions show what is possible and some say is certainly necessary now to stop cyber crimes.

What are your thoughts on these actions taken recently, and should they serve as a model for other private industries? And is there a take-away for the Department of Defense on this recent raid?

General ALEXANDER. Senator, I think it shows how we can work together, industry and Government, to do what is right here, and by bringing both of those together, we are better off for it. And I think what we have got to do is we have got to come up with that solution in this area too, and I know both bills are looking at that. And I think that information sharing is critical.

Senator HAGAN. Thank you.

General Alexander, it is often argued that terrorist groups and rogue nations, such as North Korea, for example, do not yet possess the sophisticated and extensive cyber capabilities to effectively cripple our Nation's critical infrastructure. For example, General Cartwright, the former Vice Chairman of the Joint Chiefs, has publicly expressed doubt that this class of actors could carry out such attacks today. However, we are aware of what is described as a thriving international black market where it is possible to buy or to rent cyberattack tools and large-scale supporting infrastructure such as thousands or even millions of compromised computers that are deemed to be effective against almost any type of network or information system.

This black market has developed to support the vast cyber criminal activities that have been estimated by some to now yield more revenue than the global illegal narcotics trade. This criminal money then, obviously, fuels research and development of modern and up-to-date cyberattack tools.

Could this black market in cyberattack tools and infrastructure now or in the future enable terrorists or rogue nations to acquire ready-made capabilities to inflict significant damage on the U.S. economy and our critical infrastructure? Are you worried about that?

General ALEXANDER. Senator, that is my greatest worry. And I would go beyond that group. I think the proliferation of cyber weapons, if you will, grows, that we cannot discount the actions that one smart person can do. From my perspective, when we see what our folks are capable of doing, we need to look back and say there are other smart people out there that can do things to this country. We need to look at this and say how are we going to defend. And from my opinion, that could go from—as you described accurately and I agree with it, it could be non-nation state actors all the way up to nation state actors like North Korea. I would not discount any of them. We have to be prepared for all of them. Only one of them could do tremendous damage to this country.

Senator HAGAN. Last July, General Cartwright, also speaking as the Vice Chairman, noted the challenges of recapitalizing all three legs of the triad with constrained resources. General Kehler, you have raised a similar point, that we are not going to be able to go forward with weapons systems that cost what weapons systems currently are costing today. In the search for a solution to these challenges, options seem to take the form of delaying the current programs or reducing the size of the planned programs.

What are your thoughts on the pluses and minuses of each of these options?

General KEHLER. Senator, first of all, I continue to support the need for a balanced triad of strategic deterrent forces. I think the triad has served us well. I think it continues to serve us well. I think that as we look to the future, there are attributes that are spread across the triad that continue to make sense for our national security.

Having said that, I am concerned about the costs. So I think there are a couple of things that we need to keep in mind. We need to phase these programs appropriately. We need to make sure that we have matched the investment with the needs. We need to control costs. I think there are a number of programmatic steps to take as we go forward.

When I look at the Ohio replacement program, I know that we are making decisions here today that will be with us for decades to come. The *Ohio* replacement program, as far as we can see into the future, we believe that we see the strategic need for and the strategic of a submarine-based part of our deterrent. So moving forward with that, even though we have had to delay the program some, is going to be important. That is also important with our allies, the Brits.

I think it important that we have a dual-capable long-range bomber. It needs to be nuclear capable but it will not just be used for nuclear purposes. And if we do our deterrence job right, it will never be used for that purpose. It may very likely be used to employ conventional weapons which is what B–52s and B–2s and B–1s have done. And that program is underway. I think controlling costs is going to be a big issue in both of those programs.

The next question then becomes the future ICBM, and we have begun an analysis of alternatives to look at what shape, form that might take. And then as we go to the future, I think we will get to a number of decision points on all of these systems that will allow the future environment to shape what the ultimate force outcome becomes.

Senator HAGAN. My time is up. Thank you. Both of you, thank you.

Chairman LEVIN. Thank you, Senator Hagan.

Senator Ayotte.

Senator AYOTTE. Thank you, Mr. Chairman.

Thank you, General Alexander, and thank you, General Kehler, for being here today and for your service.

General Kehler, the Senate support for the New START treaty was tied to modernization of the United States? nuclear complex and strategic delivery system. And specifically during the Senate confirmation, the President committed to modernization in what became known as the 1251 plan that was incorporated in the 2010 NDAA. Is that not right?

General KEHLER. Senator, yes.

Senator AYOTTE. And if you look at that commitment in the 1251 plan, there was an initial plan submitted in May of 2010 and then a month before the ratification of the Senate treaty, there was $4.1 billion added over 5 years to the plan. Is that not right?

General KEHLER. Yes. Are you talking about the DOD——

Senator AYOTTE. Yes. But that was specifically reflected a month before the ratification of the START treaty put into the 1251 plan as incorporated in the 2010 NDAA.

General KEHLER. Senator, I think that is right. That is a little before my time, but I think that is right.

Senator AYOTTE. And the reason that was done is because modernization was such an important issue to getting

that treaty through the U.S. Senate because modernization is very, very important for our nuclear program. Is that not correct?

General KEHLER. Yes, it is.

Senator AYOTTE. Well, the 2013 budget request underfunds the commitment made that was expressly made in conjunction with the ratification of the START treaty by over $4 billion over the next 5 years. Is that not the case?

General KEHLER. It is lower than the level of the 1251 report. Yes, it is.

Senator AYOTTE. It is $4 billion lower, roughly.

General KEHLER. I think that is right, yes.

Senator AYOTTE. Which the President a month before ratification to get the Senate to sign on to the reductions in the START treaty added $4 billion because we were so worried. I was not here at the time, but I know many of my colleagues were very worried about modernization of the program if we were going to make the reductions required by the START treaty.

And if the President is not following through, why did we not include the $4 billion in the commitment on modernization? And in particular, just to break that down, Senator Nelson had asked you about the Chemical and Metallurgy Research replacement facility. That is an 83 percent cut in that facility. In fact, we are not following through at all in our commitment to that facility. Are we?

General KEHLER. Well, the commitment has been delayed, if I understand the budget correctly. The building has been slipped to the right 5 to 7 years I believe was the number.

Senator AYOTTE. Would that not be a broken promise from what was required by the 2010 NDAA and what was specifically contained within the 1251 plan?

General KEHLER. Well, it is certainly different than the 1251 plan, yes, clearly.

Senator AYOTTE. Well, if my colleagues signed on to the START treaty concerned about modernization, with a commitment from the administration of a certain level of resources, particularly this facility that we have talked about, the CMRR facility, it is critical, is it not, to modernization?

General KEHLER. Yes, it is.

Senator AYOTTE. So no doubt that we need it to modernize.

General KEHLER. In the long run, there is no doubt we need it.

Senator AYOTTE. And so when you were being questioned by Senator Nelson, you said you owe us answers to this. Is that true?

General KEHLER. Yes.

Senator AYOTTE. I guess I would reframe it. I think what we need is a commitment from the administration to follow through on what they promised in conjunction with the ratification of the START treaty because without modernization of our nuclear deterrent, what are the concerns that you have if we do not modernize?

General KEHLER. Well, I have a lot of concerns if we do not modernize. I think you have to look at this in terms of there are four pieces to this from my vantage point anyway.

Piece number one is the delivery systems, and I just mentioned that there are modernization plans in place for the delivery systems or there is a study underway to take a look at the ICBM leg and what we might need as we go to the future.

There is command and control and the commitment to both of those.

The real issue for me is the weapons end of this and the weapons complex that supports those. In an era that we are in today, without nuclear explosive package testing where we do not do any yield testing, that puts a strain on the industrial base in a way that I believe has not been strained in the past. It strains the science and engineering skills that we have to make sure that as we do life extensions, that we have the appropriate science bases and understanding to be able to do those extensions without nuclear testing.

We have issues with aging. Most of the problems with the weapons that we have today is that they are reaching the end of their lifetimes in various stages. And so being able to have life extension for those weapons is also very important.

At the end of the day, if you have a more modern complex, we think that we probably can have a smaller stockpile because the way we would hedge against failure would be different as we go to the future.

Senator AYOTTE. But if we just reduce our stockpile and we do not modernize, are we not taking on additional risk?

General KEHLER. I think there are scenarios there where that can be additional risk, yes.

Senator AYOTTE. Well, I certainly would like to know why, as reflected in the DOD 2013 budget, the administration has not followed through on its commitment to modernization because I think that was critical, as I understand it, toward many individuals around here. They were concerned about that in the debate over the START treaty. And so it was a very important issue, and that is why it was specifically incorporated and tied to the START treaty in the 2010 NDAA. I would hope you would take that for the record and get back to us on that.

[The information follows:]

[COMMITTEE INSERT]

General KEHLER. We will certainly do that. I fully understand the concern, recognizing that nothing was immune when we went through the budget reduction to include the nuclear force. I believe that we balanced the investments in much of the portfolio. It does not look like the 1251 report, but I think we balanced much of it. What concerns me the most, I think, is the industrial complex.

Senator AYOTTE. Thank you very much.

I also wanted to follow up with a question about Russia which is—as I understand it historically, General Kehler, why did the Russians not want us to improve our missile defense system in Europe and expand it? They have been very concerned about that. Why is that?

General KEHLER. Well, I could give you my understanding of where I think they are. They are very concerned. At least in the informal contacts that I have had with some Russian officials, they continue to say that they are concerned that our deployment of a missile defense system will tip the strategic balance in our favor, that it will render their offensive capabilities irrelevant. Our contention is that is not at all true. And therein has been the conversation back and forth.

Senator AYOTTE. So my time is up.

So when the President said that essentially he had to be given space to the Russians the other day, what he was really talking about is their concerns about us expanding or enhancing our missile defense system in Europe. And even on the continental U.S., it could be interpreted that way because the Russians do not want us to do that.

So I am really concerned about that statement that Senator Inhofe asked you about in the context of what it means in terms of what we would be conceding to the Russians going forward in protecting the United States of America and our allies.

So thank you very much for appearing today. I appreciate it.

Chairman LEVIN. Thank you, Senator Ayotte.

Senator Blumenthal?

Senator BLUMENTHAL. Thank you, Mr. Chairman.

And thank you to you both for your service, your extraordinary service, to our Nation in each of your commands and responsibilities and to the men and women who serve under you.

General Kehler, if I could begin just briefly following up on a remark that you just made about the *Ohio* class submarine which you have said is going to be of strategic vital importance as far as we can see into the future. I probably am paraphrasing you, not quoting you directly. But I agree completely, and I wonder if you could speak to the significance of the Ohio class submarine replacement in terms of what its value is. How does it add value to our strategic force and why is it so important to continue building it without further delay, I should stress?

General KEHLER. Senator, each of the elements of our nuclear deterrent force brings something unique to the mixture, and the strength of the overall deterrent has always been in the sum of its parts. So as we look at this today and as we go to the future, the inherent survivability of the submarine-based deterrent has been of great value to us. It continues to be of great value as we go forward at many levels. Strategic stability is really built on survivability. The understanding that neither side possesses an overwhelming advantage to strike first, that even in the event of that kind of a highly unlikely—I mean, the world is different today and we understand that. But stability, particularly in an unforeseen crisis as we look to the future, something that would arise that would put us in crisis with any of the nuclear contenders, having a survivable element of our strategic deterrent is extraordinarily valuable. And we believe that that remains valuable as we look to the future.

Now, you can get survivability a lot of ways. An airborne aircraft is a pretty survivable platform, and if it stands off or it can penetrate or it has stealth—I mean, there are lots of attributes there that get to survivability.

But we have looked at our submarine force as providing the bulk of our survivable deterrent, in particular the day- to-day survivable deterrent. Submarines that are at sea are inherently survivable.

The issue will be with Ohio replacement is making sure it stays that way and making sure that we can deploy a platform that has those attributes that is perhaps lower in cost to operate when it is fielded, and we can guarantee, as we look to the future, that it can stay a step ahead of any developing technologies that might threaten it.

Senator BLUMENTHAL. So you would say that the commitment of our military, our Defense Department, our strategic planners is undiluted when it comes to the *Ohio* class replacement.

General KEHLER. Within the modernization efforts that we are undertaking in our strategic deterrent, this one and the long-range strike bomber are both at the top of my list.

By the way, we do not talk much about the need, but the need for a replacement tanker is equally important to Strategic Command, and that is, of course, underway with the Air Force today as well.

Senator BLUMENTHAL. Thank you.

General Alexander, I was struck by your testimony, the extraordinary insightful and helpful testimony, about the wide ranging breadth of potential cyberthreats relating to industrial espionage and intellectual property theft, as well as the potential infiltration of social media. And it reminded me of a separate and perhaps unrelated but perhaps not aspect of problematic conduct involving social media that I have highlighted recently which is the demands that employers have made for passwords, log-in information from prospective job applicants or from employees which enables them to invade the private communications, e-mails, g-chats, private accounts of their employees and potentially people with whom their employees communicate, including potentially servicemen and women or loved ones or family or servicemen and women who are applying for jobs.

I wonder if you could comment on the potential security threats apart from the invasions of privacy that may occur from the demand for information from employees about their security accounts and also what the needs are in terms of background checks on the part of your agency.

General ALEXANDER. I think, Senator, that is a great question. I think, first of all, asking for potential employees for their passwords and other things is odd from my perspective, to say the minimum.

I think the issue that I see in here is a couple things. One, how do you secure those so that somebody else does not gain access to all of them. One of the Senators had a great comment about the theft of bank records and what was going on—I think Senator Hagan about what she is seeing what Microsoft and the authorities are doing to make that easier. I am concerned about that. I am not sure about the foreign threats to this as I am to what that means to the future.

We have some tremendous capabilities in cyberspace, we as a Nation, you know, the iPads, the iPhones. And I think our people should feel free to use those and know that they are going to be protected in using them. Both their civil liberties and privacy and as a country. I think we can do both, and I think we should push for both.

This is a new area, and you can see. I mean, you are hitting right on some of the key parts when you look at how the companies are wrestling with this too. How do you provide maximum benefit without intruding. I think that is going to be an issue that we are going to wrestle with for several years.

Senator BLUMENTHAL. And when it strikes you as odd, I assume that "odd"—and it is a very well chosen word—may be a euphemism for strange or unnecessary or invasive, unacceptable.

General ALEXANDER. Senator, I am not completely up to speed on all of it. I did read it. So I do not know all the facts that go with it. My initial reaction was this does not seem right. That is what I mean by "odd." But I do not have all the facts.

Senator BLUMENTHAL. Thank you. Thank you, General, and thank you for your great work on this issue. I hope you will give thought as well—and I may ask you a question in writing about it—regarding the potential uses of the National Guard cyber units and how they can better assist you and the cost-effectiveness of building those programs through our National Guard.

General ALEXANDER. We are working with the National Guard, and there are a number of those. And I will start right with the Maryland National Guard, the Delaware National Guard, you know, go out to Washington. There are some great ones. I am sure Connecticut too. I did not want to miss that. But I do think this is an opportunity where the National Guard has some technical expertise as civilians working in this area, especially when you look in the high- tech areas. So this is something that we can leverage and we are working on that.

Senator BLUMENTHAL. Thank you very much.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Blumenthal.

Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

General Alexander, I very much appreciate the attempts you have made today to clarify the roles of the Department of Defense versus the Department of Homeland Security versus the FBI when it comes to dealing with cybersecurity. As the discussion today has indicated, I believe there is a lot of confusion over who does what and who should do what. And as you correctly said, this has to be a team approach, and DOD, DHS, and the FBI have different but complementary roles.

So what I would like to do since, based on some of the questioning I heard today, I think there is still a little bit of confusion, is just take you through a series of questions in the hopes of clarifying who does what.

First, let me say do you agree that our critical infrastructure today is not as secure as it should be.

General ALEXANDER. Senator, I do.

Senator COLLINS. And second and related to that, several studies and experts have told us on the Homeland Security Committee that critical infrastructure operators are not taking, in some cases, even the most basic measures such as regularly installing patches or software updates or changing passwords from default settings. And those are pretty basic and known vulnerabilities. Would you agree with that assessment?

General ALEXANDER. I think those are basic vulnerabilities. I would add to that we see that in a number of cases in other areas as well.

Senator COLLINS. In addition to just critical infrastructure. The reason I am focused on critical infrastructure is, obviously, if there is an attack on critical infrastructure, the consequences are so much greater than if there is an attack on one particular business even though that too can have significant economic consequences and cause many problems.

So my third question is to try to better define the roles. Would you agree that the Department of Homeland Security has the lead role in interacting with the owners and operators of critical infrastructure to get them to strengthen their protections, harden their defenses up front as opposed to when an attack occurs?

General ALEXANDER. I do agree with that, Senator.

Senator COLLINS. And the distinction that I am trying to make is once there is an attack that has significant consequences, DOD would become the lead agency just as you would if we were attacked by missiles. Is that an accurate assessment?

General ALEXANDER. That is correct.

Senator COLLINS. And there is where I think the confusion lies. It is the role of the Department of Homeland Security under the current practice of this administration and under the legislation that Senator Lieberman and I have authored to try to strengthen the defenses of our critical infrastructure. And in our legislation and in a collaborative effort with industry, which is absolutely critical that it be collaborative, the Department with industry would develop risk-based performance standards. Is that your understanding?

General ALEXANDER. That is my understanding, Senator.

Senator COLLINS. And the reason for that is to ensure that the owners of critical infrastructure implement these risk-based performance standards. But I would point out to my colleagues this is not some new bureaucracy as we have heard today. It would be a collaborative effort, and the owners and operators of the critical infrastructure would decide how to meet those standards. It would not be dictated by the Department. Is that your understanding?

General ALEXANDER. That is my understanding.

And Senator, if I could, I think that is the key point because I think the concern that I hear, that we all hear, is just that key point. How do you do this in such a way that helps industry without—I will use the term “over-regulating.” This is outside of my area of expertise, but how do you get them the standards and help them build a more resilient network, a more defensible network, if you will? That is the key to this, and I do think that is the key issue that you are wrestling with. And I think that is where we can provide technical expertise to DHS and others. And I think that is where we have got to partner with industry and just as you said. I agree with the way that you have stated that, and I think that is extremely important, that bringing the industry folks together to help decide is what I get because they want to be a player in this because this is, from their perspective, important as well.

Senator COLLINS. And in fact, we need the expertise of industry, of NSA, of DHS, of everybody working together, the results of the investigations from the FBI because this is a huge problem, and it has consequences for our national security and our economic prosperity. And it is so critical that we work together to solve this problem. And I know that is what you are committing to doing and that is what you are doing.

That is the one final point that I want to make today. NSA is already working with DHS, for example, at what is called the NCCIC, which is the 24-hour/7-day-a-week entity that has been set up. There is an exchange of personnel between DHS and NSA. Is there not?

General ALEXANDER. There is.

Senator COLLINS. And under the bill that Senator Lieberman and I have introduced, to try to get that essential visibility that you have emphasized is so important, we would require mandatory reporting in the event of an attack because this cannot be discretionary if in fact there is a significant attack on critical infrastructure. And critical infrastructure is defined as infrastructure, an attack upon which, would cause mass casualties, a severe economic impact, or a serious degradation of our national security.

So do you support requiring that mandatory reporting in such cases?

General ALEXANDER. I do, Senator, and I think I would add, as we discussed earlier, that in order for us to help prevent it, it has to be in real-time. I think that is absolutely vital to the defense.

Senator COLLINS. And the reporting and information sharing under our bill is bi-directional, as has become the latest phrase to be used in this. In other words, it is in both directions. Even NSA, the capabilities of which are unparalleled, can learn from the private sector. I think you learned that in the DIB study where there were some signatures that the private sector had that NSA may not have had. Is that accurate?

General ALEXANDER. That is accurate and logical when you think about it. Adversaries will do different things for different sectors of the Government, will use different tools for different sectors of the Government. That is one of the great things that we learned on it and how we have got to go forward on the defense industrial base pilot.

Senator COLLINS. Thank you very much.

And thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Collins.

Senator Udall.

Senator UDALL. Thank you, Mr. Chairman.

Good morning, gentlemen. Thank you for being here.

General Alexander, let me turn to you first. I have been concerned, as we all have, for some years about the potential of cyberattacks on our electricity grid here in the United States and the potential effects that such attacks would have on the critical missions, especially during an emergency or during periods of prolonged power outages.

Given the uptick of tensions in the Persian Gulf and the presence of our military in the region, I am interested to know about our potential vulnerabilities of our own military to cyberattacks in the Gulf on that electrical infrastructure that our military depends on. And I am thinking about this from the perspective of the U.S. military's reliance on fuel in the region, fuel that cannot be produced without the electricity that runs oil extraction wells and refineries and that powers pumps for offloading fuel for storage and use.

Do we have an assessment of how dependent the U.S. military in the Gulf is on electricity infrastructure? Do we have a backup plan if there were to be a prolonged grid outage? And do we understand the constitution and the vulnerability of the electricity grid in the Persian Gulf well enough to measure the effect on the oil production and transportation system especially but not limited to the oil refineries there?

Thank you for letting me direct that trio of questions at you.

General ALEXANDER. Senator, I thought you were going to ask me if I got the new iPad. I thought that is how we were going to start this out. So I did. I got the new iPad. It is wonderful.

Senator UDALL. Well, we are envious.

General ALEXANDER. That is a really good and complex question. So let me expand it, if I could, not to make it harder.

But so the underlying grids that are in the Gulf States and other parts of the region—the military will normally have backup power for military operations, generator power and other things, to operate all our critical capabilities. So for the most part, both for our computer networks and for our operations, we have backup power for our critical infrastructure.

That is not the same for the flow of oil and electricity per se throughout the region. And I think the concern that we have, the concern that I think everyone shares here is what you were driving at. Note that this is one network, one global network, with a lot of little pieces but all interconnected. So you can be anywhere on the network. My concern is not only in the Gulf but here in the United States. So as we go forward, in a crisis, no matter where it erupts, is that increasingly the probability that cyber will be part of that crisis grows and we have got to be prepared for it. And it will cover all the things that you mentioned because those are the easier things to attack and have some significant advantage for the adversary.

Senator UDALL. So you are saying we have got more work to do here to understand the potential threat and to prepare for it.

General ALEXANDER. We do. And, Senator, I think we are looking at it both from how do we defend the DOD networks. Great progress there. With Senator Collins, we just talked about defending the critical infrastructure and support to our allies. I think all of those have to be laid out and discussed. And it is growing.

Senator UDALL. And also what I was saying and I think you agreed with was the flow of oil on which the world's economy depends could also be affected by something in this realm of cyberattacks, and we need to be prepared for that in addition.

General ALEXANDER. It could be. I would not put that highest on the list. I think the electricity and the other—but you can see how that would—you know, it all depends on flow and things opening up and SCADA systems, if you will.

Senator UDALL. So SCADA systems in that part of the world are vulnerable and we are also dependent on them at the far reach of the U.S. or Europe or the Asian oil markets as well.

Thank you for that. Obviously, more attention needs to be paid to that.

Let me move to a question dealing with computer network exploitation versus computer network attack. How do you exactly draw the line between those two, and how does the Government change legal authorities funding personnel and infrastructure when moving from CNE to CNA?

General ALEXANDER. Well, CNE, computer network exploitation, is largely done under title 50. I say largely, not solely, but largely done under title 50. So that would go to the intelligence community and fall under the Executive Order 12333. While title 10 is normally where we would conduct computer network attack, you could also do it under covert action. And in times of crisis and war, our forward operating elements would operate computer network attack and exploit under title 10, and it would be done in conjunction with title 50 so the de-confliction would have to do.

The good part about training our forces together and operating together is to ensure that we can deconflict those kinds of things. And it flows back to the defense. The same thing on the defense. And that is why I think the good part about putting the defense to operate with the exploit and attack puts it as one team, not two different teams, which is what we largely had up until 2008.

Senator UDALL. So you sound as if we are well prepared to deal with those differences.

General ALEXANDER. No. I think we are well prepared to state how, Senator, we would deal with those. I think there is a lot that we have to do, and that begins with grow the force and train them. That is the most important thing that I think we can do right now.

I think the partnership with industry is critical on learning and protecting the critical infrastructure. I think those are the right steps to make.

I think all of these are in motion. I would just like to go faster.

Senator UDALL. Have we conducted—I say "we"—the U.S. Government, your command and so on—some exercises to get at this CNA/CNE hand-off, if you will, and relationship that you just outlined?

General ALEXANDER. We did have a great exercise out in Las Vegas, Nellis. Yes, outside Las Vegas. We actually never got to Las Vegas. Let the record state that.

Senator UDALL. Your iPad would have been handy in Las Vegas, by the way.

General ALEXANDER. What we did learn is just some of the things you say. While I cannot go into all of that here, it was a tremendous exercise. I will give the Air Force credit for helping to set it up there. They did a wonderful job. And we brought in all of our capabilities and our components, and some tremendous lessons learned. I think at a classified level, we could go into those. And when you see that, you would say, okay, so you are headed in the right direction. And I think, Senator, we are.

Senator UDALL. I assume I will see you in a classified setting at some point in the near future where we can discuss it further.

General ALEXANDER. I think this afternoon, Senator.

Senator UDALL. My time is about to expire. But long-term—and you may want to take part of this for the record—how do you see the relationship between the NSA and CYBERCOM evolving and changing?

General ALEXANDER. I think, Senator, they are inextricably linked. And I would put it as a platform. You do not want—any more than we want DHS to recreate an NSA, we do not want Cyber Command to recreate an NSA. So we need these two components of DOD to work closely together. NSA has got the technical talent. It has got the access, got the capability. Cyber Command will have the forces to deploy and the capability to leverage that platform and work with the intelligence side of NSA to further support the combatant commands. So I think that that relationship is growing, is headed in the right direction. I think that is one of the things that we have talked about and we both strongly agree is something that we have got to maintain.

Senator UDALL. Thank you for that.

And, General Kehler, I know my time has run out, but if you want to reply further for the record, I would certainly appreciate it. Thank you for your service as well.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Udall.

Senator Chambliss.

Senator CHAMBLISS. Thanks, Mr. Chairman.

Gentlemen, thank you for your service.

General Alexander, I thank you particularly for your recent trip down to Fort Gordon where you gave a pat on the back and a morale boost to some of the smartest, hardest working, most committed Americans who are doing a great job of helping to protect our great country. And I thank you for doing that at NSA/Fort Gordon.

General Alexander, CYBERCOM you said had 13,000 employees. Let me make sure I get this right in my mind. Actually you have 13,000 personnel under your direction. CYBERCOM itself has what? Maybe 1,000 or so personnel?

General ALEXANDER. A little under 1,000 authorized, about 900 and some, and that is not only the Cyber Command staff but also operates and directs the defense of the DOD networks. But that is correct. So what I counted in that other 12,000 is our cyber, Army Cyber Command, Air Force Cyber Command—

Senator CHAMBLISS. Various services.

General ALEXANDER. That is right.

Senator CHAMBLISS. Okay. I wanted to make sure I understood that.

NSA today does a pretty good job of intercepting and protecting the dot gov, the dot mil networks. In fact, I have heard you say that the DOD information systems are probed as many as 250,000 times an hour, over 6 million times a day from criminals, terrorist organizations, including 100 foreign intelligence organizations. And even with that huge magnitude of hacks into the system, General, NSA has done a remarkable job of protecting that system. Are you satisfied with where you are in that regard today?

General ALEXANDER. Actually I am going to answer this twice and contradict myself. We are making progress and I think we are doing a good job on it, but we are not where we need to be, Senator. And there are two reasons I say that. I do think we have the best defense right there, but it could be better, and I think for the future for military command and control it must be better. So I think the IT modernization that the Defense Department is looking at is a key part to even make it better.

Senator CHAMBLISS. The legislation that we are talking about, whether it is the administration's or Lieberman-Collins, one and the same, or the alternative legislation—neither one of those really address that issue. This is work that you are doing protecting dot gov and dot mil. Right?

General ALEXANDER. That is correct in part. If I could say, the slight difference is the information sharing of those things that we do to protect our networks that go beyond what you would normally do for a civilian network are the things that we think should be included in the information sharing parts that both of those have.

Senator CHAMBLISS. I am going to get to information sharing in just a minute.

Now, going one step further there, NSA also monitors the DIB, or the defense industrial base. And there have been numerous attempts, and it may be within those numbers that I have heard you use before. Hacks into the defense industrial base have happened, and NSA does a good job of protecting those scenarios. Where that has happened, you have been notified and you are able to respond to it. Am I correct?

General ALEXANDER. Not quite. There is an innuendo that I think is extremely important. The Internet service providers operate that. We provide them signatures, as do the other industry players, and the Internet service providers actually do the work. The reason that that is important is that I believe that is how we can scale in protecting other critical infrastructure and the mechanisms that Homeland Security and others are working with. So what we bring to the table and what FBI and others would bring is specific things that we see going on in the network that may be sensitive or classified. And so we bring that, but they actually operate it. The part that we are able to work with the DIB is to understand that they will protect and safeguard classified information. That is a key element of this approach.

Senator CHAMBLISS. My point being that your relationship with the Internet providers today allows the defense industrial base to have that protection.

General ALEXANDER. That is correct. And now it has been taken over by DHS. So they actually lead. They are the lead interface for the now DIB pilot and have been doing that for 6 weeks. We are at the table and provide technical support, but they are actually the lead on that as well.

Senator CHAMBLISS. I am looking at another what I would assume you would consider critical infrastructure, our electric grid. If the electric grid is hacked into today, there is a mechanism in place that was developed by industry where if they see something unusual, then they notify NERC and NERC immediately goes to USCERT and notifies USCERT about it, which is under the Department of Homeland Security. And they are able to provide protection to the grid under voluntary standards that the industry put forth. Am I correct?

General ALEXANDER. Yes, but I think, Senator, that is slightly different, if I could, because in those notifications, you have gone out of real time to now a part where actually we are in the forensics mode. So what they are telling is something has occurred, and by the time it gets to USCERT, what USCERT could do is not prevent it but only help them understand it.

So I think the information sharing part of what you and others have proposed would take that to a more real-time capability or at least allow that where they could say I see X happening and they, industry, could tell the Government that that event is occurring so that you could take it from the forensics side to the prevention side, which is I believe hugely important for the protection of the country.

Senator CHAMBLISS. And now coming back to what you just alluded to and you stated earlier and that is on information sharing. This is really the key, as I understand it, from the standpoint of being able to provide blanket protection to virtually every segment of the economy or every industry that wants the protection out there or that needs the protection. If they have the capability of sharing proprietary information with both the Government, as well as with other industries, like industries, then is that not the crux of what it is going to take to be able to protect all of the industrial base from a cyberattack in the short run, as well as in the long run?

General ALEXANDER. Not actually. From my perspective, Senator, the issue in this part really lies in two great capabilities. The one that we provide, I agree, they want that. They want to know what are the foreign, state, and other sensitive things that could attack them. Industry also brings together the McAfees, the Symantecs, the Lockheed Martins, and all those that work in this area, also bring a wealth of knowledge in how to configure and operate their networks to a certain standard. It is our assumption in going into this that those networks like the DOD networks would be operated to a standard. If they are not operated to a standard, then what happens is you have other ways of getting into the network that we probably are not looking at. We assume that the doors will be locked. If the doors are not locked, then somebody would get in or if the window was open. What we would be doing is looking for other types of nation state threats and assume that what I will call the stuff that the antivirus community generally sees and is working on today is taken care of.

What that means, I think, as you put all that on the table, is, one, we all have to work together and share information. I agree with that part. And I do think we have to have some set of standards. And I think that is where working with the industry, just as you said—so how do you get to that standard and how do you have the industry players work with the Government and say, so what is the right way to approach it?

As you may know, we had a meeting a few years ago with a number of the electric companies who asked just that question. So how do we do this and who is going to tell us how we work it? And I think that is the approach that we have to take, help them get there in such a way that it is not burdensome but helpful.

Senator CHAMBLISS. I think that part of both pieces of legislation is about the same. With respect to getting voluntary participation versus mandatory is a little bit different. But the fact of getting the industry to set the standards is the key, and getting the industry to share the information is the other piece of that both pieces of legislation have that is a critical part of it.

Mr. Chairman, my time is up. I did want to say to General Kehler I did not vote for the START treaty. One reason I did not is because I was apprehensive about the administration not being able to do what they said they would do on modernization. And I thank you for your specific comment on that about the fact that you are concerned about it. That is a critical aspect of this, and we look forward to working with you as we go forward. It has got to be done. Thank you.

Thanks, Mr. Chairman.

General KEHLER. Senator, thank you.

Chairman LEVIN. Thank you, Senator Chambliss.

Senator Sessions.

Senator SESSIONS. Thank you, Senator Chambliss, for that comment.

And, General Kehler, it was great to be with you yesterday and talk about some of the issues you just mentioned because the understanding that Senator Kyl had, Senator Chambliss, about the START and what kind of funding would be laid out for the next decade to modernize our nuclear weapons has not been funded and Senator Kyl was deeply disappointed about that.

Mr. Chairman, I am troubled today about this little overheard conversation between the President and Mr. Medvedev where President Obama says of all these things—overheard conversation, but particularly missile defense, this can be solved, but it is important for him to give me space. And Medvedev said I understand. I understand your message about space, space for you. This is my last election. After my election, I will have more flexibility. I understand. I will transmit this information to Vladimir.

This is not a little matter. I will tell you why it is not a little matter. We had a long debate over the missile defense. The left has never favored missile defense. President Bush was preparing to place a system in Poland. Out of the blue, it was canceled. The Pols were deeply shocked and disappointed. So were the Czechs. And we were promised do not worry about it. We will have another system when, in effect, I felt that they were trying to change the course of things, and SM–3 Block IIB, and we were going to have that, something that was not even on the drawing board then. But we were about to implant in Poland a system that we had proven, the GMD system that we had already placed in the United States.

So I guess what I say to me, the President makes us assurances that we are going to implant a new system. It will be an SM–3 system. It will protect America. Sure, we canceled that one, but we are going to build this new one. But the Russians object to the new one. They have objected steadfastly for no good reason that I can see other than maybe domestic Russian politics or use leverage against the United States.

And so now it looks like the President is saying we are going to take care of those concerns too. We are not going to build the new system. We are not going to place it there. After the election, I will take care of it, Vladimir. But that is not what he told the American people, what he told the Congress. He told the Congress we were going to build this system.

So I am worried about it. I know the significance of this little conversation, and it concerns me.

And I am also concerned that the policy of the Defense Department of the United States, when it comes to the nuclear weapons you control, General Kehler, is that we are moving to a world without nuclear weapons, the complete elimination of them. The Defense Department's nuclear posture review has 30 references to a world without nuclear weapons in it. This was directly driven by the policy of the President. He is the commander-in-chief. That is what he wanted. That is what the Defense Department put in there.

And so that is one reason Congress insisted that we budget sufficient money to modernize the aging nuclear weapons that we have. We insisted on that and it came up as a part of the New START debate. The President sent a letter to us and promised it. But it is not occurring. The money is not there.

So we are at a time of great danger, as I see it. The defense budget is under great stress. We are looking to save money wherever we can save money, and it appears to me that the administration does not have the kind of rigorous intellectual support for missile defense or nuclear weapons necessary to ensure we keep these programs on track.

So with regard to that system, let me ask you a few questions, and if you have answered these, let me know because I was ranking member on another committee that I had to attend.

Tell me about the nuclear weapons that we have for the submarines, aircraft, and so forth. You explained to me several of them were being delayed under the budget plans that you have. Would you just tell us what the budget has caused you to delay?

General KEHLER. Senator, first let me make the point that the stockpile and the deployed force that we have today I am confident is safe, secure, and effective. Those are the three watchwords that we tend to use when we are talking about this, and so today I believe that that deterrent force could meet its objectives and that it is safe, secure, and effective.

However, we have weapons that are beginning to reach their end of life. The submarine weapon—it is not classified information that the W–76 submarine weapon life extension program is underway as we sit here today. I am very encouraged by that, and the program seems to be moving forward successfully.

What the budget reductions did was it slowed the delivery of those weapons. I believe while all of these budget reductions I think in a perfect world we would say we really wish we did not have to deal with budget reductions, but the fact of the matter is that they are there and the nuclear force was not immune. So I believe that we can manage that delay in the W–76 because it is toward the end of the program that we can manage this. I think that that is manageable.

The aircraft-delivered weapons are also reaching a critical point in terms of their age. The B–61 in particular needs to go through life extension. The fiscal year 2013 budget begins that life extension effort, although it will give us the first unit, what we call the first production unit, most likely in 2019 instead of 2017, which is what the 1251 report had suggested. I believe that is manageable risk as well.

Senator SESSIONS. I would just add a political risk that when you push things out—and you are assuming Congress will act rationally and predictably in the future, but I would just say the more things are pushed out and they are not done when you planned to do them, the greater the danger is that somehow it will not happen.

But go ahead.

General KEHLER. Yes, sir. And in terms of operational risk, I believe we can manage operational risk on both of those.

We are beginning a study to look at the ICBM and remaining submarine warheads to see whether or not we can get commonality out of those as we look to a future life extension program. And we believe that there are some possibilities there. We would like to go study that and see.

So in terms of the weapons for the fiscal year 2012 budget that we are executing now that you all appropriated last year—for the fiscal year 2013 budget that is laying on the table, I believe that we can go forward with manageable operational risk.

The issue is what happens beyond 2013, and that is where the two Secretaries of Energy and Defense have said that we do not have the complete plan in place for what happens beyond 2013. That concerns me. When I look to the infrastructure, the industrial complex—and as I mentioned earlier to another question, it is a very unique, highly specialized industrial complex—the plan to upgrade the uranium processing facility remains in place. The plan to upgrade what we call CMRR, or the chemical and metallurgical building that allows us to process plutonium, is not in place. That has been slipped fairly far to the right, 5 to 7 years depending on which of the documents you look at. I am concerned about that. I am concerned about our ability to provide for the deployed stockpile, and that is my number one concern here. So I have some concerns.

We owe you answers. The two Departments are working together to look at what alternatives might exist. We are participating in that review, and as the customer, if you will, for all of this at the deterrence end of this street, I will be concerned until someone presents a plan that we can look at and be comfortable with and understand that it is being supported.

So I am not saying there is not a way forward. I am hopeful that there is. We just do not have it yet, and until we do, as the customer I am concerned and I will remain concerned until we go a little farther down the road.

Senator SESSIONS. Well, thank you. You are the customer. You are the person for whom these weapons are delivered. And you need to share with us—and I believe you have honestly—both the good and the bad news. And I think it is up to Congress to make sure that out of all the money we spend on national defense, we make sure that we have sufficient funds to maintain a credible nuclear stockpile.

So thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Sessions.

Senator Shaheen.

Senator SHAHEEN. Thank you, Mr. Chairman.

And thank you, gentlemen, for being here this morning and for your service, and hopefully I will not keep you too much past lunch.

I wanted to start, General Kehler, if I could, with talking about New START treaty implementation. As you know, the treaty was an extremely difficult and contentious debate here in the Senate, and your predecessor, General Chilton, as well as seven of the last eight commanders of STRATCOM, voiced their support for the treaty, which I think was very helpful in getting it done.

But can you tell us a little bit about how the implementation of the treaty is progressing?

General KEHLER. Senator, I can. There are a number of segments in implementation of the New START treaty that have to move forward together.

The first segment is that we need to eliminate those launchers that count against the overall treaty limits that have not been in use for a very, very long time. We call them "phantoms" simply because they count on the books, but they have been deactivated a very long time ago. Some number of bombers, B–52s are in the bone yard and need to be dismantled. There are 100 ICBM silos that have been empty now for a number of years that we do not have any plans to go back to that need to be eliminated as well, not converted from nuclear to non-nuclear, but completely eliminated. Those processes are underway. The wheels are turning. They are about to finish the environmental impact studies that go along with eliminating those silos. And so I am comfortable that those pieces are moving forward correctly.

The second thing is we have to get ourselves down to the central limits of the treaty, and that is 1,550 deployed warheads, 700 deployed launchers, and up to 800 deployed and non-deployed launchers. That requires us to select a force structure mixture and we have gone through the joint chiefs with proposals. We believe that we are settling on a final proposal that the chairman and I can take to the Secretary of Defense.

In the meantime, we have begun reconfiguration activities. We are de-MIRVing all of the ICBMs. That work has begun and it is going to continue. And we are reconfiguring the numbers of warheads on the submarines so that we can get our warheads down to certain limits. So all of these steps are underway, Senator.

I will tell you that we know that there is a clock running here. We have to be at those central limits not later than the 5th of February of 2018, and the goal we have set for ourselves is a year in advance of that so that we have time. The ICBM fields, for example, reconfiguring those—we know we will have to make some adjustments in the ICBM force. We know we will have to make some adjustments in the SSBN forces, the submarine force. There is a long lead time on being able to do that. The ICBM fields are sensitive to weather, of course, and so we have got to leave ourselves some slack. I am okay with that, but we are getting to the point now where we need to make some final force structure decisions, and I believe we are poised to make those.

Senator SHAHEEN. And so based on that, you are comfortable on the central limits that we will meet the deadlines?

General KEHLER. Yes, I am comfortable we are going to do that.

Senator SHAHEEN. And the Russians are also meeting their requirements under the treaty, as far as we know?

General KEHLER. They are.

Senator SHAHEEN. Good. Thank you.

I want to switch now to the refueling tankers because, General Kehler, as I know you have commented, one of the important support elements of the long-range bomber is obviously a refueling capability. We have seen that at Pease where we have the 157th air refueling mission, and I have had a chance to ride along on some of those planes. So I appreciate the skill and the importance of having that component.

So can you talk very briefly about how critical it is for the Air Force to modernize that refueling capability and how important it is that we have the new KC–46A tanker for those long-range bomber operations?

General KEHLER. Senator, the one word that we typically use to describe STRATCOM is “global.” That word has been used for STRATCOM since it was SAC. And so I think we appreciate the value of what makes us a global command.

In large part, what makes us a global command is our ability to project power. In large part, our ability to project power is based upon our tankers. It is not the only thing that allows us to project power. And by the way, I think that the big advantage that the entire United States military has is our ability to project power, which is why anti-access area denial counter-strategies against us are so concerning.

In that mixture, I think there is probably—when I look at my friends in Air Mobility Command and our colleagues in U.S. Transportation Command, I think there is probably no more valuable military assets that we have than our long-range aircraft that can give us strategic mobility and the tankers that make it so. So when I look at important things for us in the future, a modern tanker fleet is irreplaceable and is crucial for our success. I think that the United States? ability to project power relies on that as well. By the way, it relies pretty extensively on space and cyberspace as well for us to be able to project power.

So all these pieces go together, and anymore, it is almost impossible to say that one platform only exists in the air. They are connected by cyber. They are relayed by space. They are really truly global in nature and being able to move a lot of fuel to power projection forces is critically important.

Senator SHAHEEN. And I know it goes without saying that in addition to the equipment that is required for all of that, the skills of the human talent that is required to do that is also critical.

General KEHLER. The most critical part.

Senator SHAHEEN. Given that, one of the things that I have worked on in my civilian life before I came to the Senate was the importance of education, and obviously, one of the things that we are struggling both in the private sector now and the public sector—and I think it is particularly true in the defense arena—is making sure that we have the trained engineers, scientists, mathematicians, technicians that it is going to take for all of these jobs in the future.

So could I ask maybe if both of you might comment on what your commitment is to making sure that we have the STEM-trained people that we are going to need for the future and whether there are any particular efforts that you see that the military is involved in to help make that happen?

General KEHLER. Senator, again, having people who are STEM people who have that set of skills is irreplaceable for us. Anything we can do to support the development of our young people in that regard we need to go do. I would say it this way. In all of our combatant commands, you can look and you can see who the warriors are. Typically they are someone with a set of warfighting that you would recognize on television. They carry a rifle. They fly an airplane, et cetera. In STRATCOM—and General Alexander can speak to Cyber Command—but across STRATCOM, whether it is space or any of the other things that we do, the engineers and the scientists very often are people with that kind of background. Those are our warriors. And so it is even more magnified, I believe, in STRATCOM the value of people with that kind of background than it may be in other places.

General ALEXANDER. Senator, I would just add NSA has a program with over 100-plus universities for information assurance and cyber-related stuff. We do that in conjunction with the Department of Homeland Security, and now we bring Cyber Command into that. So that offers us a wealth. And Tulsa University was one of those that we work with, and there are many others, as you know.

But I think the issue with science, technology, engineering, and math, the STEM program, is critical for our country. And we, the military, cannot do this. It is going to take you in Congress to help generate that. We need more scientists, and we need to start that in fourth grade. And it is the things that we have absolutely got to push. I have 14 grandchildren. All of them should be engineers and scientists and mathematicians. Maybe one could be a lawyer.

Chairman LEVIN. Thank you for leaving us a little room here.

General ALEXANDER. Yes, sir.

Senator SHAHEEN. I would go for a doctor myself.

Well, thank you. I think as you point out, this is an area where the military and the civilian sector really need to work more closely than we have in the past. And I think as we talk about what we need to do in our education system, I think it is important to point out that this is a national security issue as well. So thank you all very much.

Chairman LEVIN. Thank you, Senator Shaheen.

I happen to agree with Senator Shaheen about her efforts in the STEM skills. And I happen to also agree, despite I am a lawyer and married to a lawyer, with your comment about engineers. We need a heck of a lot more of them. I will not be negative about whether we need more lawyers. I will just be positive about needing more engineers.

Both of you, we are very grateful for your comments.

The only thing I think I would add probably, General Alexander, is that you make repeated reference to what we need to do in the area of cyber in terms of working with industry. And I obviously agree with that in terms of needing performance standards. They are going to work to try to come up with performance standards. I think it is important, however, to emphasize that even though they will be adopted, that they are going to have to be followed. The industry can decide how to meet those standards but there will be standards. And I do not think you should shy away from that. I think we are talking about national security here, and this is not a question of pro-business/anti- business. This is the security of the United States we are talking about. We want to work with business, but we cannot just allow business here to dictate what the security of this country is by saying that they oppose standards. Instead, we would hope that they would work with us on those standards and understand that there is plenty of flexibility in deciding how to meet those standards, but not whether to meet those standards.

Are you with me so far?

General ALEXANDER. I am, Senator. Mr. Chairman, I agree.

Chairman LEVIN. And also another piece and that is the information sharing piece. As you point out, you want them to get to the point where they can tell us about an attack. And the bills make it easy for them to tell us because, I guess, we are addressing some of the issues about proprietary information, for instance, so that they will be protected on that.

But I think it is also clear, as your answers to Senator Collins made clear, that whether or not they share—and we are talking here about the major infrastructure in this country. Whether or not they share information with us is not a question of whether they agree to it or not. At some point, with major infrastructure there is going to be a requirement that they share information relative to attacks with us. We will protect them in terms of proprietary information, but they have got to help protect the country by understanding that there should be and I believe hopefully will be requirements that they share information of attacks on that major infrastructure with us.

I would just urge that you not be reluctant about talking about their obligation, not only that they will get to the point where they will share, but that there is a responsibility that needs to be placed upon them, and again talking here about major infrastructure, responsibility that will be placed upon them to share that information of major attacks with us.

Would you agree with that?

General ALEXANDER. Chairman, I do.

Chairman LEVIN. Okay.

Senator Shaheen, do you have anything further?

We thank you both. It has been a very, very helpful morning.

And we will stand adjourned.

[Whereupon, at 12:20 p.m., the committee adjourned.]