

**DEPARTMENT OF DEFENSE AUTHORIZATION
OF APPROPRIATIONS FOR FISCAL YEAR
2015 AND THE FUTURE YEARS DEFENSE
PROGRAM**

THURSDAY, FEBRUARY 27, 2014

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

U.S. STRATEGIC COMMAND AND U.S. CYBER COMMAND

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

Committee members present: Senators Levin, Reed, Udall, Manchin, Gillibrand, Blumenthal, Donnelly, Kaine, King, Inhofe, McCain, Sessions, Ayotte, Fischer, Graham, and Lee.

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

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

Minority staff members present: John A. Bonsell, minority staff director; William S. Castle, minority general counsel; Anthony J. Lazarski, professional staff member; Daniel A. Lerner, professional staff member; and Robert M. Soofer, professional staff member.

Staff assistants present: Lauren M. Gillis, Daniel J. Harder, Brendan J. Sawyer, and Robert T. Waisanen.

Committee members' assistants present: Carolyn A. Chuhta, assistant to Senator Reed; Christopher R. Howard, assistant to Senator Udall; David J. LaPorte, assistant to Senator Manchin; David J. Park, assistant to Senator Donnelly; Karen E. Courington, assistant to Senator Kaine; Stephen M. Smith, assistant to Senator King; Christian D. Brose, assistant to Senator McCain; Bradley L. Bowman, assistant to Senator Ayotte; Peter W. Schirtzinger, assistant to Senator Fischer; Craig R. Abele, assistant to Senator Graham; and Robert C. Moore, assistant to Senator Lee.

OPENING STATEMENT OF SENATOR CARL LEVIN, CHAIRMAN

Chairman LEVIN. Good morning, everybody. Today, we begin our annual posture hearings with the combatant commands by receiving 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 welcome Admiral Cecil Haney, in his first appearance before the committee as the Commander of the U.S. Strategic Command, and General Keith Alexander, in what may be his final appearance before the committee as commander of the U.S. Cyber Command. General Alexander also serves, as we know, as Director of the National Security Agency. And when he retires at the end of next month, he will, by far, be the longest serving NSA Director in history. And we thank you both for your extraordinary service.

This hearing comes at a time of reduced budgets across the U.S. Government, including the Department of Defense. Even though this hearing comes in advance of the 2015 budget request, we'll want to hear from our witnesses about the impact of the overall budget situation and the expected 2015 budget submission, the impact that is likely to be the result of both that overall situation and the budget submission on the programs and operations under their oversight and direction.

Admiral Haney, I hope that you will address the full range of issues impacting Strategic Command today, including the status of our nuclear deterrent, the impact of the recent ICBM cheating scandal, any potential efficiencies and cost savings that could reduce the \$156 billion that the Department projects it will need to maintain and recapitalize our nuclear triad over the coming decade, steps that may be needed to ensure that we can protect or reconstitute our space assets in any future conflict, and concerns about the adequacy of the DOD's future access to communications spectrum as pressure builds to shift more and more spectrum to commercial use.

For most of the last year, General Alexander has been at the center of both the crisis over the loss of intelligence sources and methods from the Snowden leaks and the controversy over aspects of the intelligence activities established after September 11 to address the terrorist threat. And we look forward, General, to hearing your views about the changes to the NSA collection programs directed by the President, the impact on the military of the Snowden leaks, the capability of the personnel that the military services are making available for their new cyber units, the services' ability to manage the careers of their growing cadre of cyber specialists, and steps that can be taken to ensure that the Reserve components are effectively integrated into the Department's cyber mission.

In addition, I hope that you'll provide us with your analysis of the Chinese campaign to steal intellectual property from U.S. businesses. The committee has almost completed a report on cyber intrusions into the networks of some of the Defense contractors on whom the Department may rely to conduct operations, and I hope that you'll give us your assessment as to whether China has shown signs of altering its cyber behavior subsequent to Mandiant Corporation's exposure of the operations of one of its military cyber units.

Before I call on Senator Inhofe, I want to remind everybody that we are going to have a closed session at 2:30 this afternoon to address questions from our Worldwide Threats hearing last week with General Clapper and General Flynn, questions that were de-

ferred to a closed session. We have circulated a list of those questions to committee members and to witnesses. It is my intention to go down that list that were—of questions that were deferred, recognizing each Senator on the list in the order in which the questions were raised at the open hearing. Those Senators who raised questions were Senators Reed, McCain—and this is the order that they were raised—Senators Reed, McCain, Ayotte, Blumenthal, Nelson, Fischer, Vitter, Levin, and Graham. And if a Senator lets me know that he or she is unable to attend, this afternoon, if they would like I'd be very happy to raise the question on his or her behalf.

We're also going to try to have our military noms voted on off the floor between votes. We have stacked votes, and that's a good opportunity to approve our military noms and recommend their confirmation prior to the end of the month.

So, we now call upon Senator Inhofe.

STATEMENT OF SENATOR JAMES M. INHOFE

Senator INHOFE. Thank you, Mr. Chairman.

I have the utmost respect for our panel today, for—both in the service that you've—and, I think, particularly General Alexander, because I—we've developed a close relationship, and I appreciate that very much. I think a lot of people don't realize, in that period, the time you've been here—it was touched on by the Chairman—but, been a Director of the NSA; the chief of Central Security Service; Commander, Joint Functional Component Command; the—and then, of course, the Commander of U.S. Cyber. And I—since graduating from West Point, I guess, in 1974, was it?—that you're getting close to retirement. I mean, I think you need to stretch that out now, because you're going to be retiring 39 years, 10 months. You ought to make it an even 40. Anyway. Well, any—this will likely be your last time to testify to this committee. That's a cause for celebration, I'm sure.

Admiral Haney, the 5-year debate over the course of the U.S. nuclear weapons policy is, for the most part, settled. The President, in June 2013, the Nuclear Weapons Employment Strategy is closer to the deterrence policy that has guided U.S. nuclear policy since the end of the cold war, and moves away from the President's naive vision of the world without nuclear weapons. It emphasizes the role—the vital role of nuclear weapons in deterring threats, and assures allies, it reaffirms the necessity of a modern nuclear triad as the best way—and I'm quoting now—"as the best way to maintain strategic stability and—at a reasonable cost, and hedge against uncertainty."

One of our—your challenges will be ensuring the commitment to nuclear modernization is carried out. And we'll have some questions about—specific questions about that, shortly. Congress supports these efforts. The fiscal year 2014 omnibus spending bill provided virtually all of the President's—that the President had requested for nuclear modernization. Unfortunately, the President's request fell short of the commitment that was made in 2010; that was in order to get the necessary votes to pass the New START treaty.

Energy Department funding for nuclear weapons activities over the past 3 years is about \$2 billion short, and virtually every nu-

clear weapon life-extension program is behind schedules now. The follow-on nuclear ballistic missile submarine replacement of the air-launch cruise missile are both 2 years behind schedule, and a decision on a follow-on ICBM has not been made. This needs to be addressed.

I also want to know your thoughts on the Missile Defense Agency plans to enhance the U.S. Homeland Missile Defense System by improving sensor capability and developing a new kill vehicle for the ground-based interceptor. These efforts, I think, are essential to defending this country.

General Alexander, the Cyber Command has made strides in normalizing cyber planning, the capabilities and the fielding of the cyber mission force of nearly 6,000 cyber warriors. However, I am concerned that insufficient progress has been made toward developing a strategy to deal with the growing number of complexity of threats in the—that we're facing today that we've never faced before. The status quo isn't acceptable, and the administration is to blame for its inability to develop and employ an effective cyber deterrent strategy.

Recent events show that our enemies are paying attention to well-publicized events involving Iran, one involving an enduring campaign of cyber attacks on the U.S. banks and the financial sector, and another involving the exploitation of critical Navy network. They all—should concern all of us.

So, the apparent inaction of the administration underscores its failed cyber deterrence strategy. This is going to have to change until our adversaries understand that there will be serious consequences for cyber attacks against the United States, as we've already seen coming our way.

In closing, I want to comment briefly on the Snowden situation. This man is not a whistleblower or a hero, as some have portrayed him to be. He's a traitor who stole nearly 2 million documents, the vast majority of which have nothing to do with the activities of the NSA. In the process, he's potentially giving our enemies, and also giving Russia and China, access to some of our military's most closely guarded secrets. He's undermined our ability to protect the country and has put our lives of our military men and women in greater risk. These are the hallmarks of a coward, not a hero, and it's time the American people fully understand the damage that Snowden has done to our National security.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you so much, Senator Inhofe.
Admiral Haney.

STATEMENT OF ADM CECIL D. HANEY, USN, COMMANDER, U.S. STRATEGIC COMMAND

Admiral HANEY. Good morning, Chairman Levin and Ranking Member Inhofe and the distinguished members of this committee.

With your permission, I'd like to have my full statement made as part of the record.

Chairman LEVIN. It will be.

Admiral HANEY. Thank you, sir.

I am honored to join you today as my first appearance, as was mentioned, here as the Commander, U.S. Strategic Command. I'm

also pleased to be here with General Keith Alexander, whose responsibilities as Commander, U.S. Cyber Command and Director of the NSA are critical to National Security and my command's ability to perform its missions. I greatly value his advice and counsel, and I thank him for his many years of distinguished service to our Nation.

As you know, U.S. Strategic Command executes a diverse set of global responsibilities that directly contribute to national security. And I can say with full confidence today that U.S. Strategic Command remains capable and ready to meet our assigned missions. We're blessed to have the—a talented, dedicated, and professional military and civilian workforce to address the significant national security challenges facing the United States. And I thank the Congress and this committee for your support, and I look forward to working with you throughout my tour of duty.

We appreciate the passage of the 2-year bipartisan Budget Act of 2013 and the 2014 Consolidated Appropriations Act. This legislation reduces near-term budget uncertainty. But, I remain concerned that sequestration will continue to stress the human element of our capabilities, as well as impacting our capacity to meet the threats and challenges of the 21st century.

The current global security environment is more complex, dynamic, and uncertain than any time in recent history. Advances in state and nonmilitary capabilities continue across air, sea, land, space domains, as well as in cyber space. The space domain is becoming ever more congested, contested, and competitive. Worldwide cyber threats are growing in scale and sophistication. Nuclear powers are investing in long-term and wide-ranging military modernization programs. Proliferation of weapons of mass destruction, nuclear technologies continues. Weapons of mass destruction capability delivery technologies are maturing and becoming more readily available. No region in the world is immune from potential chemical, biological, radiological, or nuclear risk. Terrorist threats remain a source of significant ambiguity, and the home—the threat of homegrown violent extremists remains a concern.

Against this dynamic and uncertain backdrop, U.S. Strategic Command's mission is to partner with other combatant commands to deter and detect strategic attack against the United States, our allies, and to defeat those attacks if deterrence fails. Our unified command plan assigned missions are strategic in nature, global in scope, and intertwined with the capabilities of our joint military force, the interagency, and the whole of government. This requires increased linkages and synergies at all levels to bring integrated capabilities to bear through synchronized planning, simultaneous execution of plans, and coherent strategic communications.

Your Strategic Command manages this diverse and challenging activity by actively executing a tailored deterrence and assurance campaign plan and by executing my five command priorities. That is to provide a safe and secure and effective nuclear deterrent force; partnering with other combatant commands to win today; addressing challenges in space; building the necessary cyberspace capability and capacity; and to prepare for uncertainty.

In keeping with the 2010 Nuclear Posture Review, my number-one priority is to ensure a safe, secure, and effective nuclear deter-

rence force consisting of the synthesis of the dedicated sensors, assured command and control, the triad of delivery systems, nuclear weapons and their associated infrastructure, and trained and ready people.

In light of recent personnel integrity concerns within the ICBM force, I fully support Secretary Hagel's initiative to assemble key Department of Defense stakeholders to fully assess and understand the implications of recent events, and seek long-term, systematic solutions that will maintain trust and confidence in the nuclear enterprise. This has my utmost attention. But, let me repeat, America's nuclear deterrent force remains safe, secure, and effective.

In addition to our critical deterrent-and-assurance work, we're engaged on a daily basis in a broad array of activities across our mission areas of space, cyber space, intelligence, surveillance, reconnaissance, combating weapons of mass destruction, missile defense, joint electronic warfare, global strike, and, of course, analysis and targeting.

While these diverse activities are being synchronized and integrated by an outstanding team, none of the work I've described can happen without trained, ready, and motivated people. They remain our most precious resource, and deserve our unwavering supporting.

My travels to a number of U.S. Strategic Command components and partner locations since I took command in November 2013 confirm my belief that we have an outstanding team in place across all of our mission areas. I have the utmost respect for their professionalism, dedication to duty, and sustained operational excellence. In today's uncertain times, I'm proud to lead such a focused and innovative team. We're building our future on a strong and successful past.

Your continued support, together with the hard work of the outstanding men and women of U.S. Strategic Command, will ensure we remain ready, agile, and effective in deterring strategic attack, assuring our allies, and defeating current and future threats.

I thank you for your time, and I look forward to your questions.

[The prepared statement of Admiral Haney follows:]

Chairman LEVIN. Thank you so much, Admiral.

General Alexander.

**STATEMENT OF GEN KEITH B. ALEXANDER, USA,
COMMANDER, U.S. CYBER COMMAND**

General ALEXANDER. Chairman Levin, Ranking Member Inhofe, distinguished members of the committee, thank you for this opportunity for what could be my final hearing here, as you stated.

Sir, I would ask that my written statement also be added to the record.

Chairman LEVIN. It will be.

General ALEXANDER. One of the things I'd like to cover, based on your questions, is a few things about what we see going on in cyber space. But, I'd emphasis up front the great men and women that we have within the Command and supporting us throughout the Department of Defense and with some of our other agencies. And I'll touch on that briefly.

You brought up the issue of the threat between—both you and the ranking member. And I think it's important to step back and look at what's going on in this space, because it impacts everything that you brought up, from what Snowden has done to where we are with our policies and laws and what we're going to do to defend in this space. It is changing so rapidly that our policy and laws lag behind it.

If you look at all the applications that are coming out and the way this space is actually growing, it is far beyond where current laws and policies have. I think this is absolutely one of the key and fundamental issues that we have to have in a discussion with the American people. How do we protect our Nation in this space and through this space? And both of those are issues that are on the table today. And how do we do it in such a manner that they know we're protecting their civil liberties and privacy while concurrently protecting this Nation?

You brought up the fact of the amount of exploits. And I'm going to define, for my use here, a difference between exploitation and the attacks. Exploitation is where their intent is to steal either information or money. And attacks will be where they want to disrupt or destroy devices or actions in and of cyber space.

We see an awful lot of exploitation. You brought up the Mandiant report and what's going on. That exploitation is for the theft of intellectual property as well as to get into some of our sensitive systems. And it goes throughout the infrastructure. From my perspective, the best way to solve the exploitation problem—and I think the—also defend against disruptive and destructive attacks—is to form a defensible architecture. JIE, the Joint Information Environment.

So, if I were to leave you with one thought of what we could and should do as a Nation, we should protect these networks better than we have them protected today. Not just within the Defense Department, but also our critical infrastructures. Time and again, we're seeing where people have exploited into these networks, only to find out that the way that they're getting in is so easy that it's difficult to defend. So, step one, Chairman, I think, is a defensible architecture.

Attacks are growing. It was mentioned by the ranking member. The attacks that we saw against Wall Street and around the world, the destructive attacks that have hit Saudi Aramco, RasGas in South Korea, and most recently, the Sands Corporation. When you look at those destructive attacks, they destroyed data on systems that had to be replaced. This is a significant change from disruptive attacks, those distributed denial of service, which only disrupt for the time that that attack is going on, versus a destructive attack, where the information is actually lost. Far more damaging, far more timely, far more costly. Both of those are going on together. My concern is, that is growing. We will see more nation-states using that. If diplomacy fails, that will be their first course. We've got to be prepared for that, as a nation, and we've got to work with our allies to set up what are the ground rules and deterrence area—in this area?

So, some thoughts. First, the Services are doing a great job, from my perspective. Working through the furloughs and sequestration,

I think where we are right now in setting up the cyber teams is superb. The training programs, I sat down with some of our folks in training. And I know several of you have asked questions on this. We have had 4,500, roughly, seats, where people have gone into different training things. One of the things that you count on me in this command is to set up the best trained force in the world. And we're doing that. We've gotten people from the Services, across the—even from the Navy, the Army, Air Force, instructors from the academies, to come out and help us set up these program. And it's superb. When you look at the number of people and the quality that we have in this, absolutely superb.

Training the young folks going in, that's going to take time. We'll have roughly one-third of that force fully trained by the end of this calendar year. And I think that, given the sequestration, is a huge step forward. And we are on track to get the team stood up, as well. They'll reach IOC, roughly one-third of those, by the end of this year. I think those are two steps forward that we've got to really focus on and that we're taking.

I mentioned team sport. Within the Defense Department, you want us to work closely with the Services. And we are, with our component commands. And that's going well. I think Admiral Haney and I see that as one of the key things that we can do, is ensure that the services are aligned and that we're training everybody to a joint standard. That's going on. We have a close relationship with them, and we operate in a joint environment. That's huge. But, we also have to work with DSSA and NSA. And I think those relationships are also good and strong.

Finally, within the interagencies, with the Department of Homeland Security and the FBI specifically, I think those relationships are good. With Secretary Johnson in place, I think we'll take some further steps forward. We'll meet with him in a couple of weeks.

Team sport, something that we have to work together. I am concerned that our policy and law lagged behind this. And part of that is educating people, the American people and our administration and Congress and the courts, on what's going on in this space. Many of the issues that we've worked our way through over the last 5 years on the NSA side, working with the FISA court, boils down to an understanding of what's going on in cyber space, our ability to articulate it, and their understanding of what we're talking about. This makes this area especially difficult, and one that I think we need to step back, set a framework for discussion with the American people. This is going to be absolutely important in setting up what we can and cannot do in cyber space to protect this country. And, from my perspective, that's going to be one of the big issues that we move forward.

I think a precursor to that is getting the NSA issues resolved. We have to get those resolved, because, ironically, it operates in the same space. If we can solve the NSA issues, especially the surveillance program that the President asked us to look for—look at, which, over the next several weeks, I think we will bring back to you all a proposal, I think that will be the first step. Pending that, we can then look at that as a way and construct for how we would move forward in cyber space.

Bottom line, Mr. Chairman, we have great people out there, the services are doing a great job. I am really impressed with the types and quality of the soldiers, sailors, airmen, marines, and civilians that we're getting. It's absolutely superb. We need to invest in that training more, and we're taking that as our top priority.

That's all I have, Mr. Chairman.

[The prepared statement of General Alexander follows:]

[COMMITTEE INSERT]

Chairman LEVIN. Thank you so much, General. If that proposal comes in the next few weeks, it may come before your retirement, in which case this may not be your last hearing before this committee. But, we would look forward to—

Senator INHOFE. Then he might reach 40 years.

Chairman LEVIN. That's true.

But, anyway, we know how much you've put into this effort, and we do look forward to that proposal. And it's way beyond this committee. The entire Congress, the American people, and, of course, the administration looks forward to the recommendations that you'll be making, or the proposal that you'll be making.

Let's have a 7-minute first round.

Admiral, you—I think you made reference to the ground-based midcourse defense—the GMD system. And we've had some flight test-fit failures with both models of the deployed kill vehicles. My question is this. Do you believe that it is a high priority to fix the problems with our current GMD kill vehicles and that we need to use a fly-before-you-buy approach to ensure that, before we deploy any additional GMD interceptors, that we need to demonstrate, through successful and realistic intercept flight testing, that the GMD system has been fixed and will work as intended?

Admiral HANEY. Senator Levin, the—very important question, there. And, as you know, the importance of missile defense system, and the ingredients that go in there—the kill vehicle is an important part of that system, and the failures that we've had in the past are under review, expecting a readout soon from the review board. But, it is critical that we get to the technical issues associated with the kill vehicle and get those corrected so that we can have better reliability in our missile defense system. That, coupled with investments in discrimination and sensors, is key to the way forward.

Chairman LEVIN. And should we fix the kill vehicle problems before we deploy any additional GMD interceptor?

Admiral HANEY. Sir, I believe we need to do both in parallel while we understand the problem deeper. And that is already underway.

Chairman LEVIN. The—General, let me shift to you about some of the issues that you addressed.

First, there was an article, yesterday's—or the day before's New York Times, saying that, in the late spring of 2011, that NSA and the Department developed options for the President to conduct sophisticated cyber attacks on the Syrian military and on President Assad's command structure. Can you provide the committee, in a classified manner for the record, if necessary, your assessment about the accuracy of the article and your views on the decision

that the President purportedly made relative to that and to the thinking behind that decision?

General ALEXANDER. Mr. Chairman, I will provide a classified response to that.

[The information referred to follows:]

[INFORMATION]

Chairman LEVIN. And you—are you—I assume you were in the middle of that discussion and those options.

General ALEXANDER. Yes, sir.

Chairman LEVIN. Okay.

General, in January, as you pointed out, the President ordered a transition to end the Telephone Metadata Collection Program, as it currently exists, to preserve the capabilities that we need, but without the government collecting and holding the data on call detail records. Do you believe that the government needs to hold all the metadata records in order to determine whether terrorist suspects overseas are communicating with persons located in the United States, or could the—a third party, a private third party, hold that data, or service providers perhaps keep the data?

General ALEXANDER. Mr. Chairman, I think there are three options on that, that I would put on the table. You mentioned government holding it, the Internet service providers holding it, and I think there is yet another option, where you look at what data you actually need, and get only that data. Can we come up with a capability that just gets those—that are predicated on a terrorist communication? I think you have those three options that I would put on the table. Those are three of the ones that I think need to be fully discussed and the merits for both sides. They have pros and cons on the agility that you would have with the programs.

I think—we have made some recommendations, and I think that will be our view down—over the next couple of weeks within the interagency. I am confident that the process is going well in this. They've had deputies and other meetings amongst the interagency, and I think the facts are being put on the table to help make a good decision to bring forward to you all.

Chairman LEVIN. The—thank you—the Privacy and Civil Liberties Oversight Board and the President's Review Group on Intelligence and Communications Technology both characterized the Section 215 program as useful; however, they said that it has not yet identified a single instance involving a threat to the United States in which the program made a concrete difference—these are their words—in the outcome of a counterterrorism investigation.

Can you, either for the record or here, give us examples or the list, if it's a finite list, of where the program made a, quote, "concrete difference" in the outcome of a counterterrorism investigation?

General ALEXANDER. Mr. Chairman, I can. There's two sets. Let me give you the first part, which was what we gave to Congress on 54 different terrorist events—not all attacks, but this could be facilitation—roughly, 13 were facilitation, and the rest were terrorist plotting and attacks—that went on here and throughout the world. That's the 54 number that everybody has known. Of those 54, 41 were outside the United States, 13 were inside the United

States. The Business Record FISA program could only apply to those 13. It actually was used in 12 of those 13.

And the issue of—so, what’s the “concrete” part, gets us back to the mid portion of this? In sitting down with the Director of the FBI, both past and present, the issue comes up with one of agility. How do we go quicker? And things like the Boston bombing shows where this program and its agility really makes a difference.

So, from my perspective, there are some ongoing, concrete examples today, that we can provide the committee at a classified, that shows, from my perspective, that this program makes a difference.

The issue really comes down to your earlier question. So, how much data do you need? How do we do this data in the right way? And can we come up with a better way of doing it? Which is what the President has tasked us to try to come up with.

I do think there is a better way. And so, that’s what we’re putting on the table. And I think it will address both of your questions—the database and how we respond.

And, Mr. Chairman, I would like to provide more details on the ongoing stuff that we’re seeing, threats that we’re seeing with this program.

Chairman LEVIN. All right, it would be very helpful that you give us the list of each instance where the program has made a, quote, “concrete difference,” because that is very different from what these two organizations and commissions found. And we’ll expect that for the record, General. We appreciate it.

[The information referred to follows:]

[COMMITTEE INSERT]

Chairman LEVIN. Senator Inhofe.

Senator INHOFE. Thank you, Mr. Chairman.

I’d ask both if you—you heard my characterization of Snowden in my opening remarks. Do the two of you agree with that?

Admiral HANEY. I do.

General ALEXANDER. I do.

Senator INHOFE. I—would someone turn over that chart over there? We’ve developed a chart that we have shown to both of you. I think, Admiral Haney, you went over this yesterday with some of our staff. And for the benefit of those up here, we have copies.

If you look at the peak there, that would have been at—as the end of the cold war came, and we started dropping down in our nuclear modernization program. And it was fairly level until getting into the—kind of the current date that we’re in right now.

You see the little hump there? That would be a new—necessary in order to get this done—a new cruise missile, new ICBM, new sub-launched. Do you—have you had a chance to look at this chart? And do you feel that’s what our needs are now, Admiral Haney, the accuracy of this chart?

Admiral HANEY. Senator Inhofe, I have seen this chart, and what I think is unique about the chart is, it really gives a great presentation of the history of funding that we have invested in our strategic deterrent, and also gives, even beyond the FYDP, an approximation of what requires to be modernized. I think, as you look at this chart, it’s unique, in terms of what was paid for, back in the late 1980s, early 1990s, and how that sustains us today in having

a credible deterrent that we're operating in a safe, secure, and effective manner today.

Senator INHOFE. Yes, well, that's kind of in the past, but the way we're going forward is what I'm interested in, which I think we're going to have to do.

Now, I—I'm going to read a list. There are eight delays that have bothered me, and I'd like to have you comment on any of these and how they fit into the chart of what our expectations of the future are.

First of all, the ballistic missile submarine, delayed 2 years; air-launch, delayed 2 years—a little bit more than 2 years; the follow-on ICBM, still no decision yet; the B-61 bomb life extension, that was delayed 2 and a half years; the—both warheads, the W-78 and W-88, delayed 2 years; plutonium handling facility, deferred at least 5 years; uranium processing facility, delayed at least 4 years; and funding of the DOE weapons activities, \$2 billion short of the New START commitments, those START commitments that were made by the President and by the administration in order to secure the votes necessary to pass New START.

Of these eight, do you—first of all, do you agree? And which do you think are more significant in correcting so that we can meet the expectations of this chart?

Admiral HANEY. Senator, you've really captured where we need to go, in terms of modernization across the triad, which—the 2010 Nuclear Posture Review, as well, articulated its value to our Nation in strategic deterrence. As I look at the modernization programs that are either in progress or going forward, clearly the—we have delayed the Ohio replacement program to the point where we can ill afford to delay it any further. Right now, those platforms are going to be the longest serving submarines in the Ohio class today, getting up to 42 years of service out of them in the current plan. And it is important that we move forward with that program.

As you look at each leg of the triad, there are modernization aspects. Some are underway. You mentioned the air leg, for example, the B-61 life extension program, there is work ongoing today associated with that program. We have to keep it on track in order to have that portion of the air leg. You know we have a three-plus-two strategy that we're committed to, and we have to continue to work that.

The one piece of this chart that has significant uncertainty gets in terms of the impacts of sequestration, particularly as we look at beyond the current fiscal year, the next fiscal year, and particularly as we look at those cuts, going forward.

Senator INHOFE. Okay. And I agree with that. But, the—part of the chart also, that most can't see from where you are, is that it would only cost—this modernization that is to reach these expectations, about 5 percent of the Defense spending. So, I see this as affordable. Do you agree with that?

Admiral HANEY. Senator, I would say to not continue the modernization of the triad is not an option. And the—this chart, though not in percentages, does, in fact, illustrate that, when you look at—in the current timeframe and—I would say, in the last 5 years we've been about 3 percent, and going up to nearly twice that much is a significant investment, but a necessary investment—

Senator INHOFE. Yes.

Admiral HANEY.—going forward.

Senator INHOFE. Thank you very much.

And, Admiral—or, General Alexander, I wanted to get into a little bit more time on this, because of my concern that I've expressed to you on several occasions, over Iran, over the threat that's there. And people think of the threat of Iran, as I have, too, as gaining the capability—a nuclear capability, a delivery system that could reach the United States. That's been a great concern of ours. But, what is not as obvious is what they—that was revealed in the Wall Street Journal article, back in February, about what they are able to successfully infiltrate the critical Navy computer network, and then, of course, getting into Wall Street and all of that. So, I'd ask you the consequences of the Iranian cyber space. And there won't be time to get into that, but I would like to have you just comment.

You were talking about the education of the American people. I think that's it. This whole thing on the NSA and how people are using an issue that may be there, but it's there only for a very small part of it. Is this what you mean when you say the education of the American people? I think that's what you mean. And again, how are we going to go about doing that?

General ALEXANDER. Mr. Chairman, that's what I mean. How do we help them understand the evolution of what's going on in this space and what the country is asking NSA to do to protect the Nation from terrorist attacks and now to provide early warning for cyber. So, you have a couple of issues that we're asking NSA to do. What we've seen with all the reviews is that they're doing it right. Everything gets pointed out that we tell the court when we make a mistake, we do it right.

But, the real issue comes down to understanding, What do we need to do to fix these problems? You mentioned access into networks. And when you look at it, it's banks, it's electric, it's government networks, it's private networks, it's all of them. And the thing that we haven't done is built security into these networks at the pace that we need to.

So, what I would propose, especially for the government, is to implement the Joint Information Environment and create a defensible architecture, and learn how to use it. We wouldn't leave our classified material out in Central Park and then wonder why people are taking it. And right now, access to these networks is fairly easy. There are a lot of ways to get into it, and they only have to find one. And that's what they're doing.

Senator INHOFE. That's right. That's right.

And my time has expired, but I talked, this morning, to the Defense Reporters Association, and told them this very thing, that people are not aware of the threat that you and I are talking about here in this hearing. And I think, as part of the educational thing, you know, we're going to have to really work on the media to properly express to the American people the reality of what we're facing and of the threat that's there.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator, very much.

Senator Reed.

Senator REED. Well, thank you very much, Mr. Chairman.

And thank you, gentlemen, for your service. Admiral Haney, welcome.

And this being General Alexander's, perhaps, last appearance before the committee, I have to thank him for his great service to the Nation. I've known General Alexander since he was a plebe and I was his company commander at West Point. And, despite that very poor initial role-model relationship, he has done quite well for himself. And I know you've been involved, General, in lots of policy questions, but no one can or should question your integrity and your selfless service to the Nation. And I thank you for that, sir. Thank you.

You've raised a series of questions, and my colleagues have, too, with respect to the intersection of threats to our commercial enterprises and threats to our National security. And these are commingling. And you're suggesting that NSA can and should play a more prominent role in providing assistance to civilian authorities, but that would require, I think, additional legislation. But, first, do we need additional legislation? And second, can you give us kind of the quick insights in what that relationship might look like?

General ALEXANDER. Senator, I'm not espousing that NSA should have a greater role inside the United States. What I am saying is that NSA has some unique capabilities in understanding threats, how they're built, and how they go about, and we should have a better relationship for how we share that, those things between government and industry. And that is where I think we need cyber legislation, sharing those capabilities, and especially those signatures.

So, let's say that we come up with a signature for how a foreign adversary is getting into our networks, and it's classified because of the way NSA got it, either through their own capabilities or through a partner. Giving it to industry in an unclassified manner would almost ensure that the adversary would know and respond and change that signature in a few days. And we've seen that happen. So, we have to have a classified relationship for sharing some of this information and technology with industry so that we can improve it.

The defensible architecture, I think that's unclassified. The way we actually defend it, that gets into a classified area. And I think that's where I believe we're going to need cyber legislation. And it's the ability to share that with industry that we'll have to legislate, because today you can't go back and forth easily.

Why I made the comment on the business record FISA is, we're also looking at, Can we share some of these terrorist selectors with industry in a classified manner and get responses back, where the government, nor anyone, has to hold an entire database? That's a possibility, and something I think we should pursue.

If we do one, if we do the business records, it sets a case in precedent for cyber, and I think that's where the public debate really needs to come down and where people need to understand exactly what we're talking about.

I would not be an advocate for having NSA operate within the United States.

Senator REED. Thank you very much, General.

One of the other sides of this discussion is that you can alert industry to potential threats, but, ultimately, industry will have to build the protection mechanisms in their systems. And that's going to require them to invest in more security. Is that—that seems to logically follow from your comment.

General ALEXANDER. Well, it—I think that's mostly correct, Senator. I would change it slightly to say there's going to be a role for government for defending the Nation so that if another nation were attacking a sector of industry, we would have the government have to step in to protect it. But, you're correct, they have to build the defensible architecture, as well, something that can tip and queue and say, "I'm having these problems, you need to step in." And those are decisions where the policy and the law have to precede the event. And that's where I think we've got to push that understanding so people understand why we have to train Cyber Command to operate at network speed in these areas.

Senator REED. Let me ask a question to both you gentlemen, and that is that the command-and-control networks, particularly with respect to our nuclear forces, which is clearly the responsibility of the government, are you confident that we successfully can protect those networks from cyber intrusion?

Admiral Haney?

Admiral HANEY. Senator Reed, yes, I am confident that we can protect those networks associated with our strategic deterrent. I do—as we look at the future of threats, I am mindful, though, that we have to keep pace, as General Alexander has discussed. And that's a necessity, because, in having a deterrent, you have to have the necessary command-and-control and communications systems that also have to be assured, not just now, but well into the future.

Senator REED. General Alexander?

General ALEXANDER. Senator, I agree, we need to—we can, today, defend it, and it's going to continue to evolve, and we have to continue that assessment and our investment in their defense.

Senator REED. Thank you very much.

All right, we've talked about the modernization issue of the triad, and we're already sort of underway in several program, but they've been delayed, as Senator Inhofe pointed out quite specifically and quite bluntly. One issue, obviously, is the Ohio class replacement, Admiral Haney, and that seems to be further along than most of the other major platforms. Is that a fair assessment?

Admiral HANEY. Senator, the requirements have been established for the Ohio replacement, and there's design work that's underway, and the plan has been going through very good detail to get us out to where we can have a commissioned platform that's certified and ready to deploy in 2031.

Senator REED. Thank you.

There's another aspect to this modernization issue, and that's not the new platforms, that's making sure that existing facilities are adequate, particularly with respect to accidental incidents. And are—you're confident, Admiral Haney, that you've—you're investing enough in just the upkeep of the facilities so that, you know, we are absolutely confident that there's—there is going to be no potential, or any significant potential, for accidents?

Admiral HANEY. Senator, my confidence exists, relative to the inspections that we do associated with our nuclear enterprise to ensure, today, that we are safe, secure, and effective. But, as you know, there are investments that are needed in some of our enterprise facilities that deal with the production, the storage, long-term storage, and dismantlement of weapons that are also required for the future.

Senator REED. Thank you very much, gentlemen. Thank you for your service.

Chairman LEVIN. Thank you, Senator Reed.

Senator McCain.

Senator MCCAIN. I thank both the witnesses.

And, General Alexander, thank you for your outstanding service. And I'm sure you view your last appearance here with mixed emotions. I would also like to congratulate you overcoming your initial schooling and malign influence of Cadet Reed. I think you've done very well.

Senator REED. Cadet Captain Reed.

Senator MCCAIN. Okay, excuse me. Cadet Captain Reed. Excuse me. Another mistake made by the authority.

But, anyway—[Laughter.]

I—General Alexander, we've been kicking around this legislation, cyber security legislation, now for several years, and we've been going back and forth. Everybody knows we need the legislation, and you've made significant and valuable inputs. I can't tell you the number of meetings I've gone to on it. And one of the biggest problems we face is that this issue crosses many jurisdictional lines of different committees. Would you—have you given thought that maybe we should have a Select Committee to examine this entire issue of cyber security?

General ALEXANDER. Senator, I think that would be a great idea, although I don't know as much about your job, unfortunately. But, I do think having something that pulls all that together would make a lot of sense.

Senator MCCAIN. And I'm sure you feel a sense of frustration that we haven't acted legislatively, which you have repeatedly over the years advocated. Is that correct?

General ALEXANDER. I am concerned, Senator, that the lack of legislation will be—will impact our ability to defend the country in this area. And—

Senator MCCAIN. I thank you.

Director Clapper and General Flynn testified that the fast majority of the more than 1.8 million documents that Edward Snowden stole has nothing to do with government surveillance programs. And it puts national security at risk, and the lives of our men and women in uniform at risk. Do you have anything to add to the—to that comment, to their comments?

General ALEXANDER. I am greatly concerned about the risk to our men and women in the military and to our Nation from terrorist attacks, because I think it is doing both. So, I would just add the terrorists.

Senator, I am concerned that they are learning how we stop them, and they're going to get through. And I think that's the near-

term issue that we face, both here in the United States and in Europe, and that we haven't adequately addressed that problem.

Senator MCCAIN. And you would agree that what's been released so far is really just the tip of the iceberg. Is that a correct assessment? That much greater damage can be done by Mr. Snowden releasing more of the documents.

General ALEXANDER. That is correct, Senator.

Senator MCCAIN. Recently, the Wall Street Journal article suggested that the Iranians were able to successfully infiltrate a critical Navy computer network. It was last February 17th that they were able to access the bloodstream of the Navy network. According to the article, Iran's infiltration of a Navy computer network was far more extensive than previously thought, and, quote, "It took the Navy about 4 months to finally purge the hackers from its biggest unclassified computer network." Do you believe we have a credible deterrence in the cyber domain against this kind of activity by Iran and other adversaries?

General ALEXANDER. Senator, I think we need to evolve a deterrence strategy that draws the lines on what is acceptable in cyber space and what actions we take. That does not yet exist.

Senator MCCAIN. And finally, I'd—maybe this is more appropriate for a closed hearing, but there's a New York Times article that said that the—Jason Healy, the director of the Cyber State Craft Initiative at the Atlantic Council, argued that using cyber warfare for humanitarian purposes in Syria, such as taking steps to degrade Assad's use of air power, might be an effective tool and one that might reverse the tide of world opinion that the U.S. Government is using cyber capabilities for nefarious ends.

Do you have a comment on that, General?

General ALEXANDER. Senator, I think one of the things that you and the administration would depend on U.S. Cyber Command and STRATCOM is to create options for policymakers to determine which is the best approach in solving these. I think that is one of the things that we've evolved. I think that's a good thing. I don't know that I necessarily agree with the statement when and how to use it. I do think other countries are using it. So, I'd go back to your earlier statement, What's the deterrence strategy, and how do we help evolve that? I think that's going to be the key to this.

I do think, in future environments, cyber will be the first tool used in future—

Senator MCCAIN. By both sides.

General ALEXANDER. By both sides.

Senator MCCAIN. As you know, General, since this probably is your last appearance, there's been a great deal of criticism about NSA spying, invasions of privacy, Americans and foreign leaders being eavesdropped on. I think I can safely say that, given your long tenure, this is probably the most controversy that's been generated about your agency and its work. I'd like to—for you to take the remaining couple of minutes that I have to maybe put this in perspective for us and for the American people.

It happens to be my opinion that we are in grave danger in a new form of warfare that most of us don't understand. And maybe you can put this in perspective for us as to what we're facing, and maybe give some response to the critics that say that we're invad-

ing every home, every individual, we are gathering all this information. You've seen it, all this publicity and controversy swirling around NSA activities. And maybe you could take a minute and try to put it in the perspective from your many years of experience in this area.

General ALEXANDER. Senator, thank you for that opportunity.

I think one of the greatest honors and privileges I've had in my 40—almost 40 years is to lead the men and women of NSA. They are the best I've ever seen, doing quietly what our Nation has asked them to do: protect this country in cyber space, and develop the tools to protect our networks. And we're doing that.

To assume that what NSA is doing is a rogue agency or is out-range, you see now, from all the different reviews, that NSA is doing exactly what the Nation has asked them to do. So, the issue now comes to a debate, What do we want NSA to do, and what do we need it to do? That gets to the heart of the issue that you've put on the table.

From my perspective, the space, cyber space, where both NSA and now Cyber Command operates, is one space where both the good guys and the bad guys all operate in that same space. Forty years ago, it was different. Foreign military communications were in a separate circuit from our domestic communications. Now they're all intertwined. And that's where the policy and the legal debates have not yet come to, I think, fruition and said, "So, how do you operate in that space so that you can stop a terrorist attack, stop a war between two countries in the Middle East, and protect this Nation?" All of that is the heart of the issues that we're talking about right now.

I think the Nation has to have NSA working with foreign partners to ensure that wars don't go on in the Middle East, that we stop terrorist attacks, and that we protect this Nation. And it's in that same space that cyber adversaries also operate in. And the rules that we have now have to accommodate both what I'll call active operators, cyber operators, and defense, from an intelligence perspective, in the same space.

I think your idea of a Select Committee, perhaps, to address this converging area is one of the things that we should look at. It is evolving quickly. And, as it will be a phase-zero to phase-one part of future conflict, we're going to have to get this right.

I think putting it—Cyber Command where it is, and what we've done with it, is the right thing. I think Secretary Gates pushing this towards NSA and Cyber Command as an entity, an activity, ensured that we had the team building it together. I think we should further evolve that team where it needs to be.

But, Senator, if I could just end on one thing. When I looked at the people of NSA and what they're doing, the true tragedy in all of this is the way the press has articulated them as the villains, when what they're doing is protecting this country and doing what we have asked them to do. And what we're finding out, in every review, in every case, they've done what we've asked them to do. And if they made a mistake, we find out, "Oh, they reported that 3 years ago to the courts, to Congress, and to the administration." No one is doing anything underhanded. They're just trying to do the job that this Nation needs them to do.

So, I think we have to have a reset with how we look at NSA and Cyber. I think we have to get on with the cyber legislation. Those attacks are coming, and I think those are near-term. And we're not ready for them. And the Nation needs an agency like NSA, with its technical capacities, to help ensure we can evolve that future space to where we need it. They're the ones, the predecessors who helped us crack Enigma, the red and purple codes from Japan, and they're the ones that helped protect our communications, and they're the ones we're going to need in the future.

So, Senator, thank you for that opportunity.

Senator MCCAIN. Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator McCain.

Senator Udall.

Senator UDALL. Good morning, gentlemen.

Admiral Haney, let me just start by saying I really enjoyed having a chance to sit and visit with you. I'm very much looking forward to, as the chairman of the Strategic Forces Subcommittee, working with you and Senator Sessions, the ranking member, and the rest of the subcommittee, to make sure that our strategic deterrent remains safe, reliable, and affordable. And we talked quite a bit about the affordability factor. But, it'll be a great privilege to work with you.

General Alexander, as always, it's good to see you. I know that you, as Senator McCain suggested, may have mixed feelings about this being your last appearance before the committee, and I, too, want to thank you for your four decades of service to our country.

That said, I remain concerned about NSA surveillance activities and the constitutional ramifications when it comes to our liberties, and I'd be remiss if I didn't address those concerns today for—at least for old times' sake. And I would add that your knowledge is vast, and I really appreciated your initial comments about how we move forward when it comes to, particularly, section 215 and 702. And I did want to make a couple of comments about sections 215, and then ask you a question.

You know well that Members of Congress, I think as long ago as 7 years, were asking questions about the use of section 215. They and I learned that we really couldn't have an open, informed debate about the law, because the official meaning of the law was secret, and that concerned a number of us. It concerned me even more when I joined the Intelligence Committee, here on the Senate side, 3 years ago, and I was able to take some time in classified settings to better try and understand what was going on.

And it felt to me like—and I believe this strongly—that secret laws undermine trust in authority, and then that erodes and damages our capacity to fight terrorism and protect the American people. And then, when the public learns that government officials have been rewriting the law in secret, confidence is undermined, and then it makes it harder for you to do the job you want to do and the job that I admire you for doing. And I believe that confidence has been undermined with regard to the Patriot Act.

So, my question to you is—and I think you'll have opportunities to answer this as a civilian, as well, because I think people are going to want to hear your point of view, given your broad experience. Do you think it was wise to keep classified the interpretation

of the law itself? And then, what advice would you give to your successor to help him understand the importance of making the boundaries of the law clear to the public?

General ALEXANDER. I think the rationale, Senator, for going in and keeping this secret was sound at the beginning. I think hindsight says, Could we and should we have done more? I think that's the open debate right now.

My concern is, now that terrorists know how we do this, do they learn such that we can't stop them? I think the real issue that I see is, we're giving them—we're giving away a capability, which means there's one less tool, or that tool at least is minimized in its capability for stopping terrorist attacks and understanding what they're up to, and for other issues like that.

I do think, though, given where we are today, we have to be transparent on this in the cyber legislation so the American people can enter into it, and that is, here's how we would propose doing this data. I think that debate that the administration would purport is one that should be open. And I think if we do that right for this set of data, we can then look at cyber legislation in a parallel effort, and do that right, as well, and in an open session.

So, I think those two would be a good way to move forward.

Senator UDALL. I want to note for the record, as well, that I hear you continuing to emphasize, "We really do need to get cyber legislation through the Congress." I also hear you implying, and I think saying directly, that we can figure out how to do the—have the right kind of approach to metadata. And again, I want to let you know I appreciate your willingness to work on that as we move forward, per the President's recommendations.

If I might, I'd like to turn to Admiral Haney and talk about the crews that operate our ICBMs. And we've been well aware of some of the stories over the last couple of months about what's been happening. I think the missile crew might pull eight alerts per month, and they spend time in the capsule, in addition to briefings, preparing for their shifts, and actually getting out to the missile field, so that a 24-hour alert actually lasts about 3 days. Again, that would equal eight times per month. And the airmen are kept very busy during their alerts, with training exercises and drills. That only leaves 6 days off a month, which is when the crews study for the exams, where they, I think, have to have a perfect score to pass.

I'm extremely concerned, you are extremely concerned, about the reports of cheating on those exams. And I fully support a thorough investigation and appropriate disciplinary action. But, there's a real need to address the root causes of some of the morale and discipline issues that have begun to surface.

Can you talk about what's done to prevent burnout in the missile crews? And—they're bright, they're talented, they're incredibly committed. How do we keep them focused on this deadly serious mission and then make sure they've got opportunities for advancement and development?

Admiral HANEY. Senator, I think those are very important questions. And these are questions that are, in fact, being looked at in the series of reviews that are ongoing, first within the Air Force in the command-directed investigation, as well as the Force Im-

provement Program, which is more of a grassroots look at this, holistically—I have people on that team, as well—in addition to the reviews that have been led by the Secretary of Defense in looking at the nuclear enterprise in its entirety.

I do believe, though, from personal experience, going down, being in the alert facilities and the capsules with our combat alert crews, though, that, through this scattering of articles, it really makes it look like that the majority of them are not dedicated to the mission. I'm here to tell you, that is absolutely false. I've met a number of these talented individuals that are very proud of serving our country as missileers in that community. And, quite frankly, they are distraught over one thing in particular, and that is their colleagues that—few of them—that have, in fact, cheated, and really feel that they are getting a broad grade instead of the grade that they deserve, because they have been carrying out this mission, day in and day out. Clearly, we are looking at the methodologies of evaluations versus certification, and working hand in hand with the Air Force to make sure we look at that hard and get it right.

Senator UDALL. Thank you, Admiral.

Chairman LEVIN. Thank you, Senator Udall.

Senator SESSIONS.

Senator SESSIONS. Thank you, Mr. Chairman.

And thank both of you. General Alexander, thank you for your service for so many years. And, Admiral Haney, we look forward to continuing to work with you and thank you for your good visit to my office recently.

General Alexander, with regard to our capabilities to intercept communications and so forth that has been discussed, NSA, the fact that that's been revealed, did it not, in fact, tell our adversaries what our capabilities are, at least some of them—most—a lot of them, and that, therefore, allowing them to avoid detection in ways that could be damaging to the United States and our ability to protect the country?

General ALEXANDER. That's correct, Senator.

Senator SESSIONS. And, in your opinion, has some of those capabilities enabled us to have information that helps protect the country from attack?

General ALEXANDER. Absolutely, Senator.

Senator SESSIONS. General Alexander, you, in a response to a previous question, said, "If DOD does not develop effective offensive capabilities in cyber space, and clear rules of engagement for using them, adversaries will have little to fear of a U.S. response and, therefore, have little motivation for restraint," close quote. In other words, as I interpret you to day, is, if they—if we have no settled philosophy about how to respond to damaging interferences with our systems through cyber attacks, then our adversaries are not likely to be deterred from adventures to try to—and damage our systems. Is that what you're saying? And how far along have we made it toward developing the kind of policies you suggest are necessary?

General ALEXANDER. Senator, I think, more specifically, we need to set the norms in cyber space, what's acceptable, what's not, and what will we do? I think the President did part of that in his 2009

paper, which said an attack in cyber space, here's what we'll respond. We'll use cyber plus everything else. I think we not only—

Senator SESSIONS. Repeat that? I couldn't—

General ALEXANDER. In his—I think, May 2009, there was a cyber memorandum that the President put out that said, "We'll respond to attacks in cyber space with cyber and any other means available." So, I think—he put that on the table. I think that's the correct approach. I think we have to take it to the next step. When and what will we do?

Right now, there are a number of things that have gone on against our infrastructure. The question is, When do we act? That's a policy decision. But, I do think what we don't want to do is let it get to the point where we find out, "Okay, that was unacceptable, and we didn't set the standard." So, I think we have to have a deterrence area. We're helping to push that.

Senator SESSIONS. So, in other words, we tell people who are causing us damage that, "When you do A, B, or C, you can expect that there'll be—you'll receive some damage in return."

General ALEXANDER. That's correct. Or some form of a deterrence area to keep them from doing that, Senator.

Senator SESSIONS. And to what extent have we gotten there? And, of course, Congress is—has a role to play in this. And we've got multiple committees in—House and the Senate, and you've got the White House and the Defense Department. Do you think we could do better to help develop a unified policy? Is that important recommendation you'd have for Congress?

General ALEXANDER. Absolutely. I think we need that. We need the cyber legislation. And, as I stated earlier, we need an—a defensible architecture. We need to implement that, as well. And, I think, share that with our industry partners so they know how to get the defensible architecture that Senator Reed talked about.

Senator SESSIONS. Well, I just—I thank you for that. And I would just say that, having been involved with the drafting of the Patriot Act—it was said it was rushed through. It was carefully done, over months of intense work. Senator Leahy, Senator Hatch, all of us on the Judiciary Committee, National Security Agency's involvement. And I believe, in virtually every aspect of the Patriot Act, what we did was carefully done so it was within the Constitution and within prior court rulings about what's permissible. And that was the goal, and I don't believe it represented, in any significant way, any kind of new erosion of American freedoms. There have great—there are great capabilities that I admit can be abused, and we need to make sure that they are not being abused, and they—and the agency needs to be watched. But, fundamentally, properly executed, I think it's not a unhealthy—a danger to our constitutional rights. And great care was taken to do that. It became a bipartisan piece of legislation that had overwhelming support.

Admiral Haney, thank you for your leadership. I believe we made some progress on some of my concerns, but I'll—I think we need to be even more clear about it. I think there's a growing consensus to maintain a strong nuclear deterrent within our government. I think you would agree with that.

Admiral HANEY. Absolutely, Senator.

Senator SESSIONS. You know, we had—the Secretary of Defense wrote a book about—signed on a book, within a year of his confirmation, on a nuclear zero—going to zero nuclear weapons. The President has talked about it. Other people have talked about it. But, that can't be in the immediate future in the world that we are living in.

So, I think that the nuclear employment strategy, the 2013 report, is pretty clear. And I hope our adversaries understand it, and American people do. It says we'll field nuclear forces to deter potential adversaries and ensure U.S. allies that they can count on America's security commitments. Is that—does that represent your understanding? And one—that's a quote from the report.

Admiral HANEY. Absolutely, Senator.

Senator SESSIONS. You think that's important?

Admiral HANEY. Very important.

Senator SESSIONS. I do, too. And it also says we'll maintain a nuclear triad consisting of ICBMs, submarine-launched ballistic missiles, and nuclear-capable heavy bombers as the best way to maintain strategic stability at reasonable cost and hedge against uncertainty. And that's one of the principles, also, in the report, is it not?

Admiral HANEY. It is not—it is definitely in the report, and it is being echoed by our leaders, Secretary of Defense Hagel, himself.

Senator SESSIONS. Well, I'm glad of that, because there's some discussion, there was some uncertainty about that, at least in my mind.

And then it says we should maintain, quote, “a forward-based posture with nuclear weapons on bombers and fighter aircraft in support of allies and partners.” That's in the report, also.

Admiral HANEY. Yes, Senator.

Senator SESSIONS. And, indeed, Secretary Hagel has said—and modernization is something, colleagues, that we really have got to get serious about. Our adversaries have a—are updating far more than we are, in many cases. He said, in January of this year, I was pleased to hear, “The modernization of our nuclear stockpile is really important,” close quote. And he went on to say, quote, “We're going to invest in the modernization we need to keep the deterrent stronger than it's ever been. And you can have my commitment on that,” close quote. So, I thank Senator—Secretary Hagel, our former colleague, Senator Hagel, and—for making that clear statement.

And I hope that you will keep us informed as you move toward accomplishing this goal of the needs and challenges that you face. And I believe Congress will respond to help you overcome obstacles, because it's just unthinkable that this nuclear system, that represents less than 5 percent of our budget, we don't do it in a way that's—that meets all the goals that we have to meet as a Nation.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Sessions.

Senator Donnelly.

Senator DONNELLY. Thank you, Mr. Chairman.

And, General Alexander and Admiral Haney, thank you so much for your service.

General Alexander, from what you've seen, what did we miss with Edward Snowden, in terms of how he got in the system, how

he got information? And, you know, when you look back at that, what happened?

General ALEXANDER. Senator, the issue that we missed here with Snowden, he was an IT specialist responsible for moving data from the continental United States to NSA Hawaii. In doing that, he had—all the data that he was moving, he had access to. So, part one is, we needed a way of tracking what he did with that data. It was supposed to go to a common sharepoint server, which he was to maintain, which it did do. But, at times, he would take that data off in a way that couldn't be seen by our sensors by the actions that he's—that he took.

Part one, we trusted the IT folks that run our networks. We shouldn't have, in this case. And, two, we didn't have enough checks and balances on exactly where that information—we fixed both of those. We've come up with about 40 different internal fixes that will help fix this whole network and make it even more secure.

I think it's depressing, from my perspective, that we have to look at defending our network from those who sit within it, that we have trusted. But, that's where we are and that's what we have to do, and that's what we're doing with the data that we have today. I think, for insider threats, we're fixing that with the way and the tools that we're putting in.

So, bottom line is, we trusted a person we should not have trusted.

Senator DONNELLY. Have you—obviously, you've made changes. You've made significant changes. Do you have an ongoing group who are looking at other areas? For instance, you looked at, in effect, this chain. Do you have groups looking at other areas in regards to worst-case scenarios and how to fix them?

General ALEXANDER. We—

Senator DONNELLY. Where there might be holes.

General ALEXANDER. Sir, we have insider threat groups that are working within the Defense Department, the intelligence community, NSA, and Cyber Command. Four different sets of those, working and sharing ideas together. I think that's a great way to red-team this approach. And we are cross-leveling those issues that we find, and working that. And I think that has been very healthy and helpful.

Senator DONNELLY. And do you see that as—you know, one of the things I was wondering is, How do we prevent it in the future? And is that it? And what else?

General ALEXANDER. So, I believe we could stop the Snowden of the future from doing what he did, the massive stuff. There will always be an issue with—we're going to have to trust some people with some level of information. We're going to have to do that. That will be almost impossible to stop, that which you take in your mind and go out with. Those parts are going to be very hard. That's where I think what we do in the court system with individuals like this will be the key way of limiting or eliminating that type of action.

So, I think we have to set a penalty system for doing this. But, that's for the courts and others to decide. From our perspective, what we're doing is, we're ensuring that people who touch the data,

we can track, audit, and ensure that they're using it correctly, and at least identify who has done something, and quickly.

Senator DONNELLY. Have you taken a look at your vetting system of people who have access to this information?

General ALEXANDER. We have. We've adjusted that, in part. But, that's a very difficult one, especially where and when a process or a person changes the way they think about something. So, we are changing the review timelines from 5 years to 2 years for different individuals, to make sure, and conducting more random checks.

Senator DONNELLY. Okay.

In another area, you had mentioned about your belief in the importance of cyber legislation. And when we looked at cyber legislation, you know, a number of folks in the business community objected to the reporting requirements that would come up. How would you assess the level of cooperation between the private sector and your efforts in protecting the networks?

General ALEXANDER. I think there—Senator, there's two sets of issues. One is, given the current Snowden issues, many of the companies want to distance themselves, in part, but understand, in the cyber area, we have to work together, we have to share. We have to understand when they're under an attack.

Ironically, we cannot see all of that. And so, the issue is, if there is an attack, especially a destructive attack, the probability that that will get through is higher in the civilian infrastructure. So, we have to have a way of sharing signatures so they can detect and stop those, and tell us when they're coming so we can go see who's doing that. And that's where FBI, DHS, NSA, and Cyber Command all work together.

Within the United States, I referred earlier with Senator Reed, I think that's something we want FBI and DHS to lead, not NSA. What we can do is provide the outside-in, telling you what's going on, who the adversaries are, and then, if the policymakers make decisions on what we can do, we have the tools and capabilities outside the country to take those actions, as appropriate.

Senator DONNELLY. One of the areas that is specialized in my home State of Indiana at Crane Naval Warfare Center is detection of counterfeit parts. And I wanted to ask you, General, What confidence do you have in our ability to detect the counterfeit or deliberately subverted components? And how are we going to strengthen our efforts to do that better in the future?

General ALEXANDER. Counterfeit part, Senator, is a tough issue, so you have to approach it two ways. One is, Where is the data going and what do we do with it? So, that gets you back to a defensible architecture, where it is the data, not the systems, that you want to take care of. I think that will help alleviate some of the concerns on these cloned or implanted parts that can do damage to our infrastructure.

It is a tough area. We have done work on that. And I can provide, in a classified session or statement, some insights to some of the things that we have done, identifying and remediating against those.

Senator DONNELLY. Okay.

And then, Admiral, I didn't want you to feel left out, here, so I had wanted to ask you—in regards to North Korea, what do you

think is needed, if anything, to shore up our anti-ballistic missile system to mitigate the threats that are being rattled on a regular basis by North Korea? And how do we make sure we're squared away there?

Admiral HANEY. Senator, as we look at North Korea as well as others, it's very important that we continue the work we've been doing in ensuring our missile defense system's reliability is the best it can be. And with that is the whole mechanism of getting to the far left of the business. This includes getting the indications-and-warning part right, as best we can, all the way to the business of improving our missile defense system—first and foremost in our ability to sense things and discriminate, as well as the business of improving our kill vehicle.

Senator DONNELLY. Thank you.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator Donnelly.

Senator Lee.

Senator LEE. Thank you, Mr. Chairman.

And I thank both of you for your many years of distinguished service.

General Alexander, we'll miss you and we have enjoyed working with you.

Admiral Haney, what is your assessment of Russian and Chinese reliance on nuclear weapons? And specifically, do you think that those countries are more likely to increase or decrease their reliance on nuclear weapon systems as a deterrent in the coming years?

Admiral HANEY. Senator, clearly we monitor closely developments in those countries regarding their nuclear arsenal. It is clear to me that both of those countries have involved—have been involved and they have publicly announced their modernization programs and some of their strategies in a variety of their legs of the—their strategic nuclear capability. I will not speculate, in terms of the future, but clearly, in terms of what we've seen to date, we have seen a definite emphasis of having a credible capability by both countries mentioned.

Senator LEE. And if—one thing I'd like to know is how any of that changes, both with regard to those countries and possibly other countries, if we, as the United States, proceed with any plan to draw down our strategic weapons below the New START levels. How is that likely to deter other countries from increasing their own reliance on nuclear weapons, on either increasing or modernizing their nuclear weapon systems? Specifically, I'd like to know what, if any, evidence exists to suggest that our drawdown of our strategic weapons would have that kind of impact.

Admiral HANEY. Senator, first, I would say that it's very important, from my perspective, that we continue to work to have a credible, safe, secure, and effective deterrent. And those actions, within themselves, are what we are about and what we are on a journey of doing, including our own modernization programs, as discussed earlier during the hearing.

The connective tissue, in terms of how other countries look at us, both from a deterrence and assurance perspective, are very important. But, I think, as they look at us today, they see us working

very hard to ensure each part of our strategic deterrent is being cared for and that are being operated in a proper manner. And, even as we go down to the agreed-upon treaty limits for New START Treaty, each warhead, to system, to systems of systems that are associated with that continue to remain a very effective arsenal to support our deterrence needs for the future.

Going beyond those limits will require negotiations and verification mechanisms, and we'll have to look at the whole thing, including tactical nukes.

Senator LEE. But, do we have any historical precedent that suggests that, as we draw down our systems, our nuclear arsenals—is there anything in our history, any historical evidence, to suggest that, as we do that, other countries are less likely to be developing, increasing, or modernizing theirs? You know, and that would include consideration of countries like Iran or North Korea. In recent years, we have drawn ours down. And so, on what basis could we conclude that continuing to draw ours down below the New START levels would likely deter other countries from continuing to move forward with their systems?

Admiral HANEY. Well, the first amount of evidence really shows the amount of nuclear stockpile that has been reduced, both from the United States of America and from Russia, in terms of treaties that have been established over the years, including the New START Treaty. Those are—

Senator LEE. But, beyond Russia, can you point to anywhere else where that's had a deterrent effect on other countries?

Admiral HANEY. I won't, at this point, try to give a thesis that connects the dots there, because the intent of each and every country is their own internal business, and I would say that countries will look at the—not just the drawdown, they will look at what's in their strategic issue—interests, and they will develop capability across various domains, including nuclear, to satisfy their needs.

Senator LEE. Okay. Okay. If we don't have a thesis on that, we don't have any evidence, either.

That does concern me, for the additional reason that, even with Russia, many of us here are very concerned with the fact that there have been reported violations, by Russia, of the INF Treaty, dating all the way back to 2008. And so, I'm interested in inquiring into your views, based on your perspective as the commander of our strategic forces, as to what the consequences are to our own national security when we have entered into a nuclear weapons agreement with a country—Russia—that's in violation of that agreement. Don't you think that that represents something of a threat to our National security?

Admiral HANEY. Senator, I think, not just my command, U.S. Strategic Command, but our whole of government takes very seriously the treaties that are in place, and give that a lot of scrutiny, in terms of things. The treaties that we have, such as New START treaty, the goodness in those is a "trust, but verify." And the verification piece is very important. When I look at what—particularly, a goodness in the New START treaty is the—it allows for more transparency than just the number of verification looks both sides have per year, and they are ongoing today, even as we work toward those New START treaty limits.

Senator LEE. Okay. Well, I appreciate your response. I'd like to submit some more questions to you, in writing, but I'd just like to leave you with the thought that I am very concerned, and I believe I'm not alone in this, in saying that it's distressing to me that we could be talking seriously about drawing down our potential in this area, even below New START levels, without evidence that doing so is going to deter other countries from developing, increasing, modernizing their own forces. I really would like to see some evidence as to why we should believe that. And that evidence certainly should extend beyond an indication that there has been some reduction by Russia, especially when Russia tends not to comply with its own obligations.

Thank you.

Chairman LEVIN. Thank you, Senator Lee.

Senator King.

Senator KING. Thank you, Mr. Chairman.

Thanks, to both of our witnesses.

Admiral Haney, I'm sitting here realizing, as we're talking about the nuclear deterrent, I wrote my senior thesis on the nuclear deterrent. I'm not going to give you the exact year, but let me just say, Lyndon Johnson was President of the United States.

What concerns me is that the premise of deterrence and mutually assured destruction assumes a state actor, a rational actor, and a non-suicidal actor. I'm wondering if we don't need to rethink the whole theory of deterrence when we're dealing with the potential, anyway, of nuclear capability in the hands of non-state actors who aren't particularly rational and who are, in fact, demonstrably suicidal. I don't expect you to give me a dissertation on this now, but I'd really appreciate some thought about the nuclear deterrent theory in an age of totally changed circumstances. Do you have any immediate thoughts?

Admiral HANEY. Senator, I will say, you know, as you look at the cost-benefit kind of relationship in nuclear deterrence, and, as you articulated, the business of the intent of the actor, rationality of the actor is important, you look at strategic deterrence in terms of what capability a nation will have that can threaten the United States of America. That's a—

Senator KING. But, we might not even be talking about nations. I think that's one of the important points, here. We're not necessarily—if Iran develops a nuclear capability, or Pakistan or someone else, and they export it to al Qaeda, you're talking about 19 people on a tramp steamer headed for Miami.

Admiral HANEY. Yes. And, Senator, that's why—and coupled with having a strategic deterrent is just as important as our efforts that are ongoing in combating weapons of mass destruction. And that part of the portfolio in the business is ongoing, too. You can't have one without the other in today's uncertain environment.

Senator KING. Well, I'd like to suggest you might follow up on this question, in terms of, What's—How does the theory of deterrence apply in 2014?

[The information referred to follows:]

[COMMITTEE INSERT]

Senator KING. General Alexander, good to see you again. We've met in a lot of committee meetings. When is a cyber attack an act of war? Any ideas?

General ALEXANDER. Well, I think that's a political decision, a policy-level decision. And I think it comes down to, What is the impact of such an attack?

In cyber space, some of the attacks will be not observable and, therefore, not a big attack. It would almost be like a show of force. Think of it as a blockade. So, you get—in cyber, you're going to have the whole spectrum that we have in the physical space now in cyber space, and I think we're going to have to learn.

But, I would submit that if it destroys government or other networks to a point that it impacts our ability to operate, you've crossed that line. Now, that's a policy decision, not mine. What we would do is recommend where those lines are.

I think those things that are less than that, that are blocking communications or doing something, think of that as the old jamming electronic warfare, now in cyber, probably less than, but it could get to an act where you want that to stop because of the impact it's having on your commerce.

So, those are issues that, what we'll call the "norms" in cyber space, need to be talked to on the international level. I think that's one of the things that we push. I think the administration is pushing those norms. I think it has to go a lot further. People need to understand it. And it gets back to some of the earlier discussions about, Do we understand exactly what we're talking about, here, by "norms" in cyber space?

Senator KING. Well, I do want to—one thought is—and, Admiral Haney, this would be for you, as well—to think about the fact that we currently, I believe, have an asymmetric advantage in this area, given the capabilities that we have. And perhaps we should develop a deterrent concept with regard to cyber, "If you mess with our networks, your lights will go off"—to provide a kind of deterrence for this kind of activity, rather than waiting for them to take down the New York Stock Exchange or the gas pipeline system; to let the world know that we have this capability, and if people want to pursue this activity against us, they will be retaliated against in a way—and, indeed, the nuclear deterrent theory worked for 70 years. So, I just commend that to you as a possible American strategic statement.

I just—Mr. Chairman, I want to associate myself with the comments of Senator McCain. I've been, now, to a lot of hearings here and in the Intelligence Committee that have focused on the necessity for cyber legislation. As you know, there was a major bill in 2012 that failed, and here we are, a year and a half later, every one of our witnesses has told us how important this is, how urgent it is, and yet, for reasons that I'm not entirely clear on, we aren't there yet. And maybe we need a Select Committee to iron out differences between Intelligence, Judiciary, Armed Services, whoever, to get this on the floor.

If we have an attack, 2 or 3 months from now, and we haven't done anything, we're going to look pretty dumb around here, because we've certainly had plenty of warnings in every one of these hearings. And I think it's time that the Congress acted. I don't

think it's a particularly partisan issue, and I hope that we can figure out a procedural way to move forward. And I thought the suggestion Senator McCain made, made some sense, of putting together some kind of Joint or Select Committee in order to do this.

Final question. Admiral Haney and General Alexander, should Cyber Command be elevated to a full unified combatant command? Are we at that stage in the evolution of this threat?

General ALEXANDER. I think we're getting towards that stage. What I would say right now, what we've done great with STRATCOM is set up the command, get the people trained. We're going to get to a point where you have enough forces, where I think unity of command, and the command and control between Secretary and the President directly to that, will make more sense. And I think, from an operational perspective, that's something that they will need to consider probably over the next year or so. I think, with those teams coming online, that goes great.

I would just say, candidly, General Bob Koehler and Admiral Haney have been superb to work with, so it has not risen to an issue. I do get concerned that, if there is an attack, having a streamlined command-and-control from the White House to that command is going to be important, and you're going to want to have something like that. So, I think you're going to get to that over the next year or so.

Senator KING. I think the next Pearl Harbor is going to be cyber, and I certainly hope that we're going to be prepared, better prepared than we were in 1941.

Admiral HANEY. Senator, as General Alexander has stated, we work, our two organizations, very closely together, and we recognize the speed of cyber. The one thing I would say connecting the dots to all of your questions—when we look at deterrence and our capability, sometimes we like to slice and dice it into one particular area versus the other. Our whole-of-government and our full military and national capabilities are what adversaries have to look at, in terms of deterrence at large. And that can't be lost as we drill into specific areas. And even as we look at what command-and-control organization we have in the future, the real key will be how we interconnect all of our different areas together in order to prevent, deter, and, if deterrence fails, to get at it and win.

Senator KING. I appreciate that, but, again, given our asymmetric advantage in cyber, it seems to me that we are in a position now where we could use it as a deterrent to any kinds of—any of these kinds of activities.

I appreciate your testimony, gentlemen.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator King.

Senator Fischer.

Senator FISCHER. Thank you, Mr. Chairman.

Thank you, General, for your service. I appreciate the many years that you have served to protect this country and our citizens.

And welcome, Admiral Haney. It's good to see you. I appreciated having the opportunity, just about a week ago, to be back in Nebraska, and you were very kind, and we had a number of briefings there at STRATCOM, and I appreciate you taking the time to do

that with me, and look forward to many more in the future, and congratulate you on your new command.

You mentioned the defense of nuclear command-and-control networks from cyber attack. Can you talk more generally about the need that we have to modernize those systems?

Admiral HANEY. Senator, as we have talked before, but, in particular, when we look at strategic deterrence, the business of having both the correct sensing of the environment and the ability to move the information such that we have the appropriate command and control in a timely manner is critical. So, this is an area that we continue to work on, will continue to have investments. We have a strategy that we're working to move forward on. We have to stay on course, even with sequestration.

Senator FISCHER. You know, a lot of times we focus on the hardware, on the platforms. We talk about the need to modernize warheads, the costs of our bombers and submarines. But, how are we going to communicate all this? What about our phone lines? What about the new building that's going up there in Bellevue, on Offutt? Can you talk a little about the importance of all that?

Admiral HANEY. Senator, I would say, in the command-and-control structure, what we count on is redundancy and reliability through a spectrum of different adverse environments. When you look at the different missions that U.S. Strategic Command has—I do thank the Congress for their investment in the command-and-control complex that's being built, because our ability to command and control our forces as well as move information is important. And this goes all the way to the forces, those folks in either alert facilities, bombers to submarines, all the way up to the President of the United States.

Senator FISCHER. We heard questioning from Senator Lee and then from Senator King about deterrence, and if it is effective. We still face threats from nations who have nuclear capability. So, I believe that that deterrence is extremely necessary. But, since we also face the threat from terrorists and from others, there's that—to me, that natural tie-in with cyber security being necessary and making sure that our country is prepared in that respect, as well.

I know, in the past, there's been the talk about separating the two command authorities, and the necessity of doing that. Do you think that's the way to go? In my conversations with General Koehler in the past, just looking at how the—how it works and how we're able to make those decisions by one commander, I think leaving it under one command, maybe at this point but also in the future, makes sense, especially with our budgetary constraints. I would ask both of you—I know, General, you just spoke about possibly, in a couple of years, maybe separating them. But, I would ask the Admiral's opinion on that, as well.

Admiral HANEY. Senator, I think myself and General Alexander are in fundamental agreement that what we want to do is win in cyber, and we want the command-and-control structure that allows us to win, first and foremost. As we look at investments to be made, as General Alexander has spoken and discussed, it's most important that we build up our cyber capability, and that's the piece that's a priority for me, as well. So, as I look at investment dollars in the near term, very important to build that capability.

And we may get to a point, at some point, where our National leaders fundamentally believe that that's the best organization, and we—to change structure, it's got to be the structured to win.

Senator FISCHER. General, do you have any comments?

General ALEXANDER. I agree, and I think what Admiral Haney said is right on target.

The—just to help articulate one step further, let's say an action was going on in the Middle East that didn't yet get to the strategic. You also then have and want us to directly support that combatant command in those actions. And we both do.

The issue that I see that's really going to raise this is, cyber is more likely to be used in what we call phase zero. And so, the continuity of command and control from phase zero to phase one is where I think we'll actually start to look at, How do we do this?

From my perspective, what Admiral Haney put out there, the most important thing we can do right now is train and organize those teams. And that's where we're focused. I do think this is something that we'll wrestle, post my time here. I just put that on the table as a logical conclusion from my perspective from about a year, year and a half out.

Senator FISCHER. Thank you both very much.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator Fischer.

Senator KAINE.

Senator KAINE. Thank you, Mr. Chair.

And, to our witnesses, appreciate this important testimony.

To open off with a question, really for both of you—Admiral Haney, you said, you know, the question of what is the right command structure is subsumed under the goal, which is, we want to win in cyber. And winning in cyber, I focus on our personnel. Do we have the personnel to win in cyber?

Admiral Haney, in your testimony, you noted that plans call for 133 cyber mission teams manned by over 6,000 highly trained cyber personnel by the end of fiscal year 2016. And I'd like to have each of you talk about the challenges of the recruitment and training of these—of, you know, specialized cyber personnel in an economy where they have a whole lot of other options. Talk a little bit about that dimension of the challenge that we face.

General ALEXANDER. So, Senator, let me just start off. We are actually getting good feed from the services in this area. So, from—by the end of this year, we'll probably be one-third of the way through, even with sequestration, in terms of bringing them on board and getting them into training seats. As you would expect, the training in these programs, depending on which position on the team they're going to, goes from anywhere from 20 to 40-some weeks, plus. So, that's the key, if you will, the big problem that we have, is getting them through that. That's 4,600 different courses, course seats, that we'll have had people in by the end of this year. So, the services have done extraordinary work.

In terms of hiring these people in, from my perspective, the young kids coming in, they want to do this. This is great, and they're great people. Some of our best operators in this space are the military personnel. We've got to continue to do that.

We need to look at how we encourage them to stay in the military. That's going to be incentive pay and things that we've talked to the Services about. But, my hat's off to the service chiefs who have helped push this in our Service components. I think, by the end of this year, where you see where we are, and if you have a chance to come up and see some of those teams in action, actually doing real-world missions, it's superb. It is exactly what our Nation needs them to do, both on the offensive preparation side and protecting our infrastructure.

Admiral HANEY. Senator, I have also watched and had an opportunity to chat with some of our cyber warriors, not as many touch points as I'm sure General Alexander has had. And I often ask this question to them. What makes them stay on? And it is being able to contribute to the mission that makes a difference, to a point, they're—every time I've asked that question. So, I'm proud of each and every one of them and what they do.

I will say, also, we focus a lot on that portion of the business, but there's also planning that goes on, associated with cyber, and that's integrated in terms of what our combatant commands do, geographically, across the globe, and that's the fusion of our capability, cyber with our other capabilities, that also make a difference as we go forward.

Senator KAINE. I would expect that, within the cyber space, you have an interesting mixture of Active Duty military and DOD civilian personnel. Is that profile the mixture of—in the service branch and then civilian DOD sort of different in your cyber work than it is in other military missions?

General ALEXANDER. It's roughly the same, Senator.

Senator KAINE. Okay.

General ALEXANDER. And the services approach it a little bit different. We gave them some different leeway. But, I think the key in the cyber civilian area—one of the things that we're looking at is, How do we put all the team onto a same footing for their personnel system so that they're not disadvantaged, each in different ones. So, we have CCP, ISSCP, MIP, service ones.

Senator KAINE. Right.

General ALEXANDER. But, what you really want is them to be one team. So, how do we help them do that? That's something that we're looking at and, I think, a key point.

Senator KAINE. And remind me that, earlier in 2013, when we faced sequestration, do different parts of your unit get affected differently, whether they were civilian, DOD, or Active Duty?

General ALEXANDER. Well, that specifically was the problem. So, many of them had to stand down or furlough on one side, because they were in one side of billets, while others were allowed to stay on because they were in a different set of billets, and then the military, yet different. So, it did tend to separate and cause problems, within the team, that I would like to fix. I want them to think of themselves—they're here for the good of the Nation as a cyber team. Erase those budget boundaries, if you would.

Senator KAINE. General Alexander, there were some reports in February 2014, just recently, about Chinese People's Liberation Army in Shanghai and how they employ thousands of members specifically trained to conduct cyber attacks against critical infra-

structure in the United States—power grid, gas lines, water works. Talk a little bit about—if you would, just about the magnitude of the cyber effort underway in the People’s Republic of China that you are basically trying to defend the Nation against every day.

General ALEXANDER. Senator, to get into details on that, I’d like to answer that in a classified setting, if I could. I would just tell you, you hit on the key parts. We have a lot of infrastructure—electric, our government, our financial networks. Look at all the ways that we’re—look at what happened to Target and others. So, when you look at it, it covers the whole spectrum.

We have to have a way—a defensible architecture for our country, and we’ve got to get on with that. We’ve got to look at how we take away from adversaries an easy ability to penetrate that—steal intellectual property, money or other things. So, that’s JIE, but JIE, where we give it out to others. I think we’ve got to get with that.

In terms of what China and other nations are up to, I’d rather answer that in a classified session so I don’t make a mistake.

Senator KAINE. Understood. Understood.

Let me ask Admiral Haney a question. One of STRATCOM’s ongoing tasks—and your testimony discusses this on pages 20 and 21—is work on the Syrian chemical weapons disposal together with European Command and the Defense Threat Reduction Agency. There are some professionals and assets in Virginia that have been engaged in this. The Cape Ray is a Merchant Marine ship based out of Portsmouth that’s currently in Rota, that has been involved in this. And we have intelligence professionals at Ravana Station that have been involved through the DIA, as well. Talk a little bit about the work that STRATCOM does in this ongoing effort to rid Syria of one of the largest chemical weapons stockpiles in the world.

Admiral HANEY. Senator, this is obviously an ongoing effort that involves, not just U.S. Strategic Command, but, as mentioned, the European Command as well as the international organization. So, OPCW, for example. And that piece, it’s good to see the teamwork that’s going on together with other allies and partners that are contributing to this mission. It was—from a Strategic Command standpoint, working with our Strategic Command Center for Countering Weapons of Mass Destruction—that’s also at the DTRA headquarters—has been instrumental in working to come up with a solution to rid ourselves of some of those chemical weapons by the facility that’s built on Cape May, as you discuss. That’s a good-news story, but that’s part of the story, in terms of the collective international effort that’s ongoing in order to rid Syria of those chemical weapons.

Senator KAINE. Right.

Mr. Chair, thank you.

Chairman LEVIN. Thank you, Senator Kaine.

Senator Graham.

Senator GRAHAM. Thank you, Mr. Chairman.

General Alexander, I wish you well in retirement, but I wish you were not retiring. You’ve done a great job for our country, and I find you to be one of the most capable officers we have, and I just

want to let you and your family know how much I appreciate your service to our country.

Now, having said that, could you describe, in 30 seconds—and I think what Senator King and Kaine talked about, just boil it down—what would a—what could a major cyber attack do to the United States? What kind of damage could incur?

General ALEXANDER. I think they could shut down the power in the Northeast, as an example, Senator, shut down the New York Stock Exchange, damage data that's in the Stock Exchange, remove data, shut down some of our government networks, other government networks, impact our transportation areas. Those are things that—

Senator GRAHAM. Release chemicals?

General ALEXANDER. I think that would be harder. They could get into SCADA systems, and we—

Senator GRAHAM. Affect water supplies?

General ALEXANDER. Water supplies, right. They could do damage to that. They could do flows on rivers.

Senator GRAHAM. Would it cost us trillions of dollars?

General ALEXANDER. Potentially, especially in the financial sector.

Senator GRAHAM. Could it cost thousands of lives?

General ALEXANDER. Could.

Senator GRAHAM. And you're telling us Congress hasn't given you and your colleagues the tool to deal with this threat. Is that fair to say?

General ALEXANDER. That's correct, Senator. We need a way to work with industry to understand this.

Senator GRAHAM. Well, if all this could happen, and we could help, seems like we would. Do you agree with that?

General ALEXANDER. I agree, Senator.

Senator GRAHAM. And when it comes to bipartisanship, I would allow Senator Whitehouse to write the bill. I've been in a bipartisan coalition with him. I think he's one of the smartest people in the Congress who understands this issue. So—

General ALEXANDER. He's superb.

Senator GRAHAM. Isn't he? I mean, he really—I hate to say that about Sheldon, but he really—[Laughter.]

I'll just limit it to cyber. I don't want to hurt him, back home.

Senator INHOFE. That would be more appropriate in closed session—[Laughter.]

Senator GRAHAM. Yes, probably. That's probably—you're right. You're right.

Now—so, in your tent of sequestration, if we continue down the road of what we're doing to our military and our intelligence community, what kind of effect will that have on our ability to defend ourselves in your world, General Alexander?

General ALEXANDER. Senator, the key thing that it would impact is our ability to train and get these forces in. That's where I see the biggest impact. What happened last year when we had sequestration and furlough, it knocked out the training for about 6 weeks, which actually restarts a lot of that training. Set us back—

Senator GRAHAM. On a scale of 1 to 10, how much capability would we be losing in your area if we allowed sequestration to be fully implemented?

General ALEXANDER. I'd have to go back to get an accurate answer on—

Senator GRAHAM. Would it be catastrophic?

General ALEXANDER. It would be, in my opinion. I just don't know, Senator.

Senator GRAHAM. We'll give that a 10.

Admiral Haney, if sequestration is fully implemented, what kind of effect does it have on your ability to modernize the force?

Admiral HANEY. Senator, in—if sequestration is fully implemented, it will have a—potentially disastrous impacts, in terms of things. It really will be all up, in terms of the critical decisions that would have to be made, in terms of with the—the money that is allocated and appropriated by this—

Senator GRAHAM. So, let me see if I can summarize your testimony. If the Congress continues on the path we have charted regarding sequestration, we'll have a catastrophic effect on the intelligence community, we'll have a dangerous effect on our ability to defend the Nation through strategic weaponry. On the cyber front, you've described a Pearl Harbor on steroids, and you're asking Congress to act. So, let's just remember what's been said today, that we have to do something about sequestration, in my view; we need to do something on the cyber front.

Now, let's get back to Senator King's questions, which I thought were very good, about the role of strategic forces. Do you agree with me that deterrence is one aspect of a strong, capable nuclear program to deter rational nation-states from engaging the United States? Is that still a viable concept in the 21st century?

Admiral HANEY. Yes, Senator, it is.

Senator GRAHAM. Do you agree with me that what Senator King said is true, they're—people who embrace chaos and suicide will not be deterred. So, our goal, when it comes to terrorist organizations and rogue states who do not, you know, have a rational bone in their body, is to deny them the capability.

Admiral HANEY. That's correct, Senator. And—

Senator GRAHAM. Do you agree with me, General Alexander—this is where you come into play, big time—the idea of a nuclear device coming into the United States on a steamer with 20 people on board is not a thing of novels. Is that a real threat?

General ALEXANDER. That's one of our great concerns, Senator.

Senator GRAHAM. And do you agree with me that that's one of the real things the NSA can do to help the country defend itself, to find that out before it happens?

General ALEXANDER. I do, Senator.

Senator GRAHAM. Prevention, denial, and interdiction. So, we need to make sure that, when it comes to rogue states, who will not act rationally when it comes to terrorist organizations, that we can have good intelligence, we can stop it before it starts.

Now, when it comes to Iran, do you believe they're a rational nation-state, in terms of owning nuclear weapons? Would you feel comfortable with the Iranians having a nuclear capability?

General Alexander.

General ALEXANDER. Senator, I would not.

Senator GRAHAM. Admiral Haney.

Admiral HANEY. I would not, as well.

Senator GRAHAM. Would one of your great concerns be that they would share that technology with a terrorist organization?

General ALEXANDER. Senator, what—that's part of my concern, and/or use it.

Senator GRAHAM. Either way, it's not a good outcome.

Can you envision a circumstance if there's a deal struck with the Iranians, General Alexander, that allows them to enrich uranium, even at a small level? What's the likelihood that Sunni Arab states would want light capability?

General ALEXANDER. I think it's probable.

Senator GRAHAM. Could somebody actually ask the Sunni Arab world, "What would you do if the United States agreed to allow the Iranians to enrich, at any level?" Do you agree with me, Admiral Haney, that one of the nightmare scenarios for the world would be if you had enrichment programs over uranium all over the Mid-East?

Admiral HANEY. Senator, I would agree and state that one of our aspects of deterrence and assurance is working to prevent just that.

Senator GRAHAM. So, I would end with this thought. If somehow, some way, the world sanctions an Iranian enrichment program, you have set the stage for the whole MidEast to becoming an enrichment zone, and God help us all, under that scenario.

Thank you.

Chairman LEVIN. Thank you, Senator Graham.

Senator Ayotte.

Senator AYOTTE. Thank you, Mr. Chairman.

I want to thank both of you for being here and for your extraordinary service to the country. Thank you, General Alexander. You know, and you've done a wonderful job and have had to serve during very challenging times, so appreciate your service; and your service, as well, Admiral Haney.

I wanted to follow up—let me just follow up on the Iranian threat. Admiral Haney, when DNI Clapper came before this committee last year, he said that the Iranians were working on two systems, ICBM systems, that would give them the capability of hitting the United States of America by 2015. Where are we on that threat, in terms of the Iranians' ICBM program and their capability of hitting the United States?

Admiral HANEY. Senator, I would really want to address that question in a more classified forum to get to the real details necessary to answer that question. But, the prediction—or the assessment to 2015 remains, from my understanding.

Senator AYOTTE. So, the—so, DNI Clapper's assessment—public assessment last year, of 2015, still stands at this point, from your understanding. I understand you don't want to get into the details of that in this setting.

Admiral HANEY. Yes, Senator.

Senator AYOTTE. And so, you know, one of the threats that obviously—Senator Graham asked you about the threat of perhaps the Iranians with their nuclear program, if it is permitted to continue—is to provide that technology to terrorist organizations. But,

obviously, the ICBM threat is one that we would be concerned about, as well, to our country. Would you both agree?

Admiral HANEY. Yes, Senator.

General ALEXANDER. Yes.

Senator AYOTTE. And we're—we also faced, as we've talked about in this hearing, a threat from the North Korean ICBM capability, as well, correct?

Admiral HANEY. Yes, Senator.

Senator AYOTTE. So, one of the issues that we have been discussing in this committee is the issue of a third missile site, an east coast missile site for protection of the east coast of the United States of America. And in the defense authorization, we have asked for a contingency plan for that site. I wanted to get your sense of where that stood and how quickly, if we made the decision to go forward with an east coast site, would it take us to stand that up, in light of the fact that we're facing a potential threat of 2015 by the Iranians? And you would agree with me that the east coast site would provide additional protection against that kind of threat.

Admiral HANEY. Senator, an east coast site will definitely provide additional capability against a threat, to augment what we already have. But, as we have discussed, fundamentally we have to invest in priorities order to work to get our sensing and discrimination right, as well as getting our kill vehicle also performing to spec. But, the current system provides us some capability.

Senator AYOTTE. Some capability, but yesterday General Jacoby testified before the HASC, and he said that the third site, if you built it, would give us better weapons access, it would give us increased inventory and increased battlespace with regards to a threat coming from the Middle East. And those are the facts. So, you would agree with him on that, that this—if, in fact, we are facing an Iranian ICBM threat, in addition to further sensing and discrimination capabilities, this would be important, given the population centers we have—New York, Washington—to have that additional, as General Jacoby described it, increased inventory and increased battlespace.

Admiral HANEY. I agree 100 percent with General Jacoby on increased inventory and battlespace.

Senator AYOTTE. Are you working with General Jacoby on the contingency plan if this Congress makes the decision to go forward with that site, so that we're ready to do it?

Admiral HANEY. We are working the planning associated with that.

Senator AYOTTE. Excellent. Thank you.

How do you assess, right now, the threats that we face from North Korea—I know you were asked about it earlier, but where do you assess our ability, particularly—I know that we're adding the additional groundbased interceptors in Alaska, but how do you assess our ability to meet that threat, as well, at the moment? And where are we in installing those additional interceptors in Alaska?

Admiral HANEY. The work is ongoing for those additional interceptors to be complete by about 2016. But, there's other work that's ongoing across our missile defense apparatus. Things that we have done, for example, the THAAD capability that was placed in Guam, the work we're doing to get a second TPY-2 radar in Japan, busi-

ness of upgrading our sensors, and the work to improve discrimination, all ongoing to help with this capability, including getting to the next test associated with our system—our groundbased system.

Senator AYOTTE. And that would be the next test, to ensure that the kill vehicles are properly working, given the prior tests and the assessment of those tests?

Admiral HANEY. That's correct, Senator.

Senator AYOTTE. So, one of the things that Senator Inhofe asked you up front that I think is of concern to many of us is the modernization commitments that were made by the administration under section 1251 in conjunction with signing the New START treaty. And, just to put it in simple terms, Where are we? And how do you assess the resourcing of those modernization commitments, both now, in the current fiscal year 2014 budget context, and then going forward, in particular on those modernization commitments? Obviously, with—if sequestration were to stay in place, that's one scenario. And then, if you can give us a real sense of, Where are we on this? Because I remain deeply concerned that those commitments are not there at the level of resources that they should be, making sure that we have the modernization that needs to be done to our nuclear deterrent.

Admiral HANEY. Senator, the modernization efforts, some of which are definitely in progress and in a good place, some of the work that has been going, in terms of three-plus-two strategy associated with warheads, is moving forward. Clearly, there's had to be a prioritization of efforts and a relook at certain efforts to ensure affordability and cost-effectiveness. And that piece is ongoing, as well.

Senator AYOTTE. But, as we look at this—these issues—I know my time is up, but the one thing I think of is, What keeps you up at night in this position? Both of you. I know you're—I'm—to me, I think that's the most important thing we should be thinking of. What are you most worried about? We may not ask you the right question.

Admiral HANEY. Well, my biggest concern right now is we're looking at the future, and particularly our ability to balance resources and be able to, at the same time, work to have credible capability across the spectrum in all the mission areas that I have responsibilities for as combatant command, in addition to the strategic nuclear deterrent, maintaining that in the safe, secure, and effective manner so, as mentioned, that our assurance prevents other countries from wanting to increase their—or go nuclear, in terms of capability.

Senator AYOTTE. I'm afraid to get this answer, General Alexander. What keeps you up at night? But—

General ALEXANDER. Sure.

Senator AYOTTE.—please share that with us.

General ALEXANDER. Yeah. So, there's two issues. We talked about cyber. So, that's half of it. The other is in the terrorism area. I think the greatest concern that I have, both for our country and for Europe, is a terrorist attack that galvanizes some of these Islamic fundamentalists into a true fighting force that could hurt our Nation and Europe. And I believe, right now, we don't have the proper footing, especially with our European allies, to stop that. We

have to have a candid set of discussions, solve our own problems with business record FISA and other things. But, we've also got to deal with them to ensure that they're doing something similar to protect themselves.

In the past, as the President pointed out, we do a lot to help protect them. Some of our capabilities have been impacted by these leaks. Our ability to stop it has gone down just when they're growing. So, look at Syria, Iraq, all of that. And I am concerned, over the next 12 months, something like that bad will happen.

Senator AYOTTE. Thank you both. Thank you for your service. We really appreciate it.

Chairman LEVIN. Thank you very much, Senator Ayotte.

Does anyone need a second round? [No response.]

I'm going to withhold my questions for a second round. Instead, I'll be asking both of you some questions for the record, which we'll expect prompt answers on.

[The information referred to follows:]

[COMMITTEE INSERT]

Chairman LEVIN. And we will stand adjourned.

[Whereupon, at 11:50 a.m., the committee adjourned.]