S. HRG. 114–772

OPEN HEARING: NATIONAL SECURITY AGENCY ACTIVITIES AND ITS ABILITY TO MEET ITS DIVERSE MISSION REQUIREMENTS

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

THURSDAY, SEPTEMBER 24, 2015

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
29–493 PDF WASHINGTON : 2018

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

RICHARD BURR, North Carolina, *Chairman*
DIANNE FEINSTEIN, California, *Vice Chairman*

JAMES E. RISCH, Idaho
DAN COATS, Indiana
MARCO RUBIO, Florida
SUSAN COLLINS, Maine
ROY BLUNT, Missouri
JAMES LANKFORD, Oklahoma
TOM COTTON, Arkansas

RON WYDEN, Oregon
BARBARA MIKULSKI, Maryland
MARK R. WARNER, Virginia
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
MAZIE HIRONO, Hawaii

MITCH MCCONNELL, Kentucky, *Ex Officio*
HARRY REID, Nevada, *Ex Officio*
JOHN MCCAIN, Arizona, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*

CHRIS JOYNER, *Staff Director*
DAVID GRANNIS, *Minority Staff Director*
DESIREE THOMPSON-SAYLE, *Chief Clerk*

CONTENTS

SEPTEMBER 24, 2015

OPENING STATEMENTS

WITNESS

SUPPLEMENTAL MATERIAL

OPEN HEARING: NATIONAL SECURITY AGENCY ACTIVITIES AND ITS ABILITY TO MEET ITS DIVERSE MISSION REQUIREMENTS

THURSDAY, SEPTEMBER 24, 2015

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 2:32 p.m. in Room SH–216, Hart Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Present: Senators Burr, Feinstein, Risch, Coats, Rubio, Collins, Lankford, Cotton, Wyden, Warner, King, and Hirono.

OPENING STATEMENT OF HON. RICHARD BURR, CHAIRMAN, A U.S. SENATOR FROM NORTH CAROLINA

Chairman BURR. I'd like to call this hearing to order.

Admiral, welcome. I'd like to welcome Admiral Rogers, Director of the National Security Agency. Mike, as you well know, we typically hold our hearings in closed session so that we can review your classified programs. Given the sensitive nature of these programs and the need to protect sources and methods by which intelligence is gathered, that position is certainly understandable. Today, however, we want to take time to ensure that the American people have an opportunity to learn more about the NSA, the mission your workforce is tasked with, and what you're doing to combat the increasing cyber threat to our Nation.

Cyber threats to our U.S. national and economic security are a top priority for the intelligence community, and destructive cyber intrusions and attacks are increasing in scale, scope, complexity, and severity of impact. The Office of Personnel Management recently suffered from one of the biggest cyber breaches our government has ever encountered, and there are countless other recent examples of cyber breaches and attacks in both the public and the private sector.

While NSA typically works in secrecy, I think all of us on this Committee expect that you'll be front and center on the issue for the foreseeable future, informing and educating the American public.

I'd like to take a moment to thank you and your workforce for your dedication and the critical work you continue to do to protect our Nation. You are by now accustomed to the different and direct questions which we ask you often in closed session, and you know

that we do so to challenge you and your organization always to be better.

Admiral, today represents a unique opportunity for you to educate the American people on what you do, how you do it, how your agency's postured to address the growing cyber threat for both state and non-state actors.

I want to thank you again for joining us and I look forward to your testimony as you seek to separate the myth of the NSA from the reality of the NSA, to the extent you can do so in an open setting, and we recognize how different that is.

I would also respectfully remind my colleagues to avoid any questions that touch on classified programs or questions that would require Admiral Rogers to divulge any sensitive information, and the Vice Chair and I will consult if in fact we believe that we've put Admiral Rogers in that type of situation.

Again, welcome, Admiral. I turn to the Vice Chairman.

OPENING STATEMENT OF HON. DIANNE FEINSTEIN, VICE CHAIRMAN, A U.S. SENATOR FROM CALIFORNIA

Vice Chairman FEINSTEIN. Thanks very much, Mr. Chairman, and thanks for holding this open hearing to allow the Committee to discuss in public the important work that the NSA does and some of the current challenges they face to keep up with national security threats against us.

Director Rogers, welcome back before the Committee. As we have discussed many times in closed sessions, NSA and Cyber Command are at the forefront of a number of major national security challenges and policy decisions. So I look forward to this discussion today.

Before getting to the rest of my statement, I want to publicly praise the work the NSA has done in collecting intelligence that has enabled the rest of the government to identify and stop terrorist plots directed or inspired by the Islamic State of Iraq and the Levant here in the homeland. This threat is by no means over, but there have been a number of important disruptions thanks to good intelligence and good law enforcement work, and you figure in that in a major way. So thank you very much.

As FBI Director Jim Comey noted in his testimony before our Committee in July, and I quote: "The foreign terrorist now has direct access into the United States like never before." End quote. There are now more than 200 Americans who have traveled or attempted to travel to Syria to participate in the conflict and that remains a significant concern.

I'd appreciate your assessment of the ISIL threat and the threat to the United States from others as well. Of course, when discussing that threat we also have to recognize that, due in part to leaks of classified information, improved operational security by terrorist groups, and the availability of encrypted means of communications that cannot be collected, there is increasingly a limit on what NSA will be able to contribute. I know we'll have a chance to discuss that change.

There are also numerous press reports in the past week or two suggesting that the Administration is rethinking its support for any legislative solutions to this problem. We welcome your

thoughts on how to approach the so-called "going dark" issue. I think the more you can tell the public about it here today, the better.

Certainly, the hack on the OPM database, as the Chairman said, demonstrates the need for better protection of personal information. But I'd very much like to hear your views on whether this is an either-or situation or if there's a way to keep private communications protected while still allowing the government to gain access to critical information when it's doing so pursuant to a court order or other appropriate legal process. As the head of one of the most technically proficient agencies in the government, your input into this question is very important.

Next, while the Committee has been following the implementation of the USA Freedom Act, today presents a good opportunity for the American public to hear how that transition is going. Under the new law, the NSA will no longer collect phone metadata directly from phone companies and conduct its own tailored queries of those data. Instead, the government will have to obtain a court order in order to ask telecommunications providers to query their own records and produce the responsive information.

It's important, I think, for the public, as well as for us, to know whether this transition will be complete at the end of a 180-day period and whether you assess, if the system is in place at that time, if you assess it will meet your operational needs.

I'd also like to know whether this system, once fully in place, will achieve the goal of providing NSA with responsive information from a broader set of records than it had before the USA Freedom Act passed or whether there will still be the relatively small percentage of phone records that were available to you before the change.

Finally, you've briefed the Committee recently on the reorganization you're putting into place in the NSA. It would be appropriate at this hearing for you to describe that reorganization to the extent that you can, why it's needed, and what changes are being made.

Again, thank you very much for the work your agency does. I've been very proud of it, and thank you for your leadership.

Chairman BURR. Thank you, Vice Chairman.

For the purposes of Members, we will skip the one-question round for this open hearing and we'll go to five-minute questions after the Admiral has testified. We will do that based upon seniority, which I'm sure Senator Wyden and Senator Risch will complain to me about since they're on time today and typically they might be running a few minutes behind.

But with that, Admiral Rogers, the floor is yours. Again, welcome.

STATEMENT OF ADMIRAL MICHAEL S. ROGERS, USN, DIRECTOR, NATIONAL SECURITY AGENCY; COMMANDER, U.S. CYBER COMMAND; AND CHIEF, CENTRAL SECURITY SERVICE

Admiral ROGERS. Thank you. Chairman Burr, Vice Chairman Feinstein, Members of the Committee: Thank you for inviting me today. It's a distinct honor and privilege to appear before you. I appreciate this opportunity to speak to you about the National Secu-

rity Agency, about who we are, what we do, and how we contribute to the Nation's security. In talking with you, moreover, I'm grateful for this chance to explain to the American public whom you represent what it is that their fellow citizens at NSA do to defend our Nation as well as support allies and partners around the world.

NSA plays a critical role in protecting the United States' national security systems and providing insightful and actionable foreign intelligence to our leaders, military commanders, and foreign partners. We're the Nation's cryptologic arm and America and her allies depend on our efforts.

The NSA workforce, approximately 40,000 civilian and military employees, is headquartered at Fort Meade, Maryland, just outside Washington, as you know. We have facilities in 31 states and a global presence that spans the world. The team that I am proudly a member of comprises a diverse group of individuals who come from every corner of America. About 40 percent of our team is uniformed military, representing every service, with both active duty and reserve members. Our team members at NSA include analysts, collectors, operators, mathematicians, linguists, cryptographers, engineers, computer scientists, and too many other skills to list here by name.

Our workforce ranges from high school interns to junior enlisted members of the military to senior executives of the civilian service and flag-rank officers in the military. NSA personnel are well educated, with over 75 percent of our civilians holding bachelor's degree or higher. Our military and civilian linguists working in our foreign intelligence mission have proficiency in over 120 different foreign languages. Almost 40 percent of our employees work in the science, technology, engineering, and mathematics fields, and they hold the majority of the over 200 patents that have been granted to members of the NSA workforce, more patents than any other Federal agency.

In addition to working every day to keep our country safe, our employees help to enhance their local communities by doing things like volunteering in classrooms, planting community gardens, and helping to clear the Appalachian Trail. They donate thousands of gallons of blood to the Red Cross every year, contribute millions of dollars to Federal charity drives, and give tons of food to the "Feds Feed Families" hunger drive. NSA and its affiliates are volunteer firemen, Marines collecting for the "Toys for Tots" campaign, Airmen serving with the Civil Air Patrol, Soldiers coaching Little League, Sailors volunteering to clean the Chesapeake Bay, and civilians leading Girl and Boy Scout troops. In short, they are your neighbors.

NSA employees work hard and they work well to keep our Nation safe and protect our civil liberties and privacy. Let me explain their main duties and missions in a little bit more detail. NSA's Information Assurance mission—Information Assurance mission—is to protect national security systems, such as systems that process classified information. We generate ideas for defending these networks and impart valuable security insights so the public and our allies may benefit. In short, we ensure that our Nation's leaders and military can communicate securely and that adversaries cannot gain access to our Nation's secrets. That work also enables us

to develop new opportunities to share warning and cyber insights with the private sector, so America can improve the overall security and integrity of its information systems and critical infrastructure.

NSA has evolved with changes in technology as the world has shifted from analog to digital communications, following the emergence of networks and the convergence of devices and functions in our modern mobile society. As a result, NSA now plays a key role in cyber space, assisting U.S. Government efforts to see, mitigate, and deter cyber security threats. In concert with public, private, and foreign partners, our work helps to ensure users, operators, and administrators maintain control of their systems and data.

NSA also gives our leaders unique insights into the hostile activities of foreign powers and their agents. Our people lead the Nation's signals intelligence enterprise, defending America and our allies by collecting, analyzing, and reporting foreign intelligence and counter-intelligence information derived from the interception of foreign signals and communications. NSA does this work in accordance with law and strict guidelines, and only by collecting foreign intelligence in response to specific requirements from U.S. policymakers and senior U.S. commanders which are deemed necessary to advance the Nation's policy goals to warn and report on strategic and military developments around the world and to prevent strategic surprise.

What NSA collects and analyzes is driven by the priorities listed by our Nation's political and military leaders in formal and constantly reviewed tasking documents. We work within a framework of law, rules, and oversight provided by Congress, the Executive Branch, and, as appropriate, the courts. That system of accountability ensures the privacy and civil liberties of U.S. persons.

On a daily basis, NSA provides insights into hostile plans and intentions so that our customers and partners can counter threats across the globe. Our military and its partners rely on NSA to help them achieve tactical and operational success. Our products are part of the fight, as essential to military operations as food, fuel, and ammunition.

Our requirements include a wide range of SIGINT missions. One of our most important SIGINT missions is counterterrorism, discovering terrorist plans, intentions, communications, and locations to disrupt and defeat their attacks. As a combat support agency, NSA directly supports the military with information to perform its missions and to provide force protection, indications and warning, and over watch support to keep our troops out of harm's way.

Our work also helps the United States and its allies to capture bomb makers, spot illicit fund transfers, work transnational crime, and explain to other nations how terrorists hope to transit their territory.

We also work to identify potential threats to U.S. citizens, military personnel, and embassies around the world. In addition, we devote considerable resources to the international campaign to halt the spread of weapons of mass destruction, tracking, reporting, and sharing data to keep nuclear, biological, and chemical weapons out of the wrong hands to keep the Nation safe.

We also assist the efforts of the Department of Homeland Security to protect America's critical infrastructure from cyber attacks.

Finally, we support U.S. Cyber Command, which I also lead, and will continue to help the Command develop the capability and capacity it needs to accomplish its vital missions.

As you well know, the threat environment both in cyber space and in the physical world is constantly evolving, and we must keep pace in order to maintain our advantage and generate the insights that our Nation is counting on. Our Nation's networks, communications, and data are increasingly at risk from diverse and persistent threats. These include rogue states, organized criminal enterprises, and terrorists, who are showing a willingness and an aptitude to employ sophisticated capabilities against us, our allies, and indeed anyone who they perceive as a threat or a lucrative target.

Various self-proclaimed cyber activists also cloud the threat picture. In addition, certain states are disposed to conduct cyber coercion against their neighbors and rivals and to fund campaigns of cyber exploitation against us and our allies. The targets of their efforts extend well beyond government and to privately owned businesses and personally identifiable information, putting the privacy and data of all Americans at risk.

Terrorist tactics, techniques, and procedures continue to evolve. Those who would seek to harm us use the same internet, the same mobile communication devices, and the same social media platforms that we all use in our everyday lives. As terrorists become more savvy about protecting their communications, we must keep pace in order to protect the Nation and our allies.

NSA will continue to rise to these challenges. As an enterprise, we have had to reinvent ourselves before and we will do so again. The use of intelligence to protect our Nation dates back to the United States' very origins during the Revolutionary War. NSA's predecessors, working with their World War II partners, found German U-boats by solving Enigma machine messages. They helped turn the tide of the war in the Pacific at Midway by cracking the Japanese codes.

Today the men and women of NSA fight terrorists around the globe. Today we target the communications of terrorist organizations who mean to do us harm, helping to uncover and thwart their efforts to communication with sleeper cells around the world or recruit fighters to their cause. The means of communications have changed, but the requirement to maintain our ability to collect and exploit the communications of hostile foreign actors remains constant.

When the information revolution transformed communications, NSA helped lead the way towards information assurance and pioneered intelligence in cyber space, while enabling military and counterterrorism operations in real time, in full compliance with the Constitution and the law. Every NSA employee takes an oath to preserve, protect, and defend our Constitution and its civil liberties and the privacy of our citizens that the Constitution guarantees. We just repeated this oath across our workforce on 9–11. Security and privacy are not tradeoffs to be balanced, but complementary imperatives, and NSA supports both.

The complex issues before us today represent an opportunity to write yet another chapter in our agency's rich tradition of service to the Nation. NSA plays an indispensable role in enabling our

leaders to keep the peace and secure the Nation. Our value lies in facilitating positive outcomes for the Nation and our allies, and we have delivered this for well over 60 years. Our unique capabilities are more in demand and more important to the Nation's security than ever. We are rightfully proud of that accomplishment and what we continue to accomplish, and we are striving to ensure that the American people take pride in NSA.

Mr. Chairman, Madam Vice Chairman, and Members of the Committee: Thank you again for the opportunity to be here with you today, and I look forward to your questions.

[The prepared statement of Admiral Rogers follows:]

Testimony of
Admiral Michael S. Rogers, USN
Director, National Security Agency
Chief, Central Security Service
before the
Senate Select Committee on Intelligence
24 September 2015

Chairman Burr, Vice Chairman Feinstein, and Members of the Committee, thank you for inviting me. It is a distinct honor and privilege to appear before you today. I appreciate this opportunity to speak to you about the National Security Agency/Central Security Service (NSA/CSS) – about who we are, what we do, and how we contribute to national security. In talking with you, moreover, I am grateful for this chance to explain to the American public whom you represent what it is that their fellow citizens at NSA/CSS do to defend our nation as well as support allies and partners around the world.

NSA/CSS plays a critical role in protecting the United States' national security systems and providing insightful and actionable foreign intelligence to our leaders, commanders, and partners. We are the nation's cryptologic arm, and America and her allies depend on our efforts.

The NSA/CSS workforce, approximately 40,000 civilian and military employees, is headquartered at Ft Meade, Maryland. We have facilities in 31 states and a global presence at locations around the world. The team that I proudly lead comprises a diverse group of individuals who come from every corner of America. Almost half of our team is uniformed military, representing every Service, with both active duty and reservists. Our team members include analysts, collectors, operators, mathematicians, linguists, cryptographers, engineers, computer scientists, and too many other skills to list here. Our workforce ranges from high school interns to junior enlisted to Senior Executives and Flag rank officers. NSA/CSS personnel are well educated, with over 75% of our civilians holding bachelors' degrees or higher.

Our military and civilian linguists working in our foreign intelligence mission have proficiency in over 120 foreign languages. More than a third of NSA/CSS employees work in the science, technology, engineering and mathematics (STEM) fields, and they hold the majority of the over 200 patents granted to members of the NSA/CSS workforce – more patents than any other Federal agency.

In addition to working every day to keep our country safe, our employees help to enhance their local communities by volunteering in classrooms, planting community gardens, and helping to clear the Appalachian Trail. They donate thousands of gallons of blood to the Red Cross every year, contribute millions of dollars to Federal charity drives, and give tons of food to the "Feds Feeds Families" hunger drive. NSA/CSS affiliates are volunteer firemen, Marines collecting for the Toys for Tots campaign, Airmen serving with the Civil Air Patrol, Soldiers coaching Little League, Sailors volunteering to clean the Chesapeake Bay, and civilians leading Scout troops. In short, they are your neighbors.

NSA/CSS employees work hard and well to keep our nation safe and protect our civil liberties and privacy. Let me explain their main duties and missions in a little more detail.

NSA/CSS' Information Assurance (IA) mission is to protect national security systems, such as systems that process classified information. We generate ideas for defending these networks, and impart valuable security insights so the public and our allies may benefit. In short, we ensure that our nation's leaders and military can communicate securely and that adversaries cannot gain access to the nation's secrets. That work also enables us to develop new opportunities to share warning with the private sector so America can improve the overall security and integrity of its information systems and critical infrastructure. NSA/CSS evolved with changes in technology as the world shifted from analog to digital communications,

following the emergence of networks and the convergence of devices and functions in our modern, mobile society. As a result, NSA/CSS now plays a key role in cyberspace, assisting U.S. government efforts to see, mitigate, and deter cybersecurity threats. In concert with public, private, and foreign partners, our work helps to ensure users, operators, and administrators maintain control of their systems and data.

NSA/CSS also gives our leaders unique insights into the hostile activities of foreign powers and their agents. Our people lead the nation's signals intelligence (SIGINT) enterprise – defending America and our allies by collecting, analyzing, and reporting foreign intelligence and counterintelligence information derived from the interception of foreign signals and communications. NSA/CSS does this work only in accordance with law and strict guidelines, and only by collecting foreign intelligence in response to requirements from US policymakers that our leaders deem necessary to advance the nation's policy goals, to warn and report on strategic and military developments worldwide, and to prevent strategic surprise. What NSA/CSS collects and analyzes is driven by the priorities listed by national political and military leaders in formal and constantly reviewed tasking documents. We work within a framework of law, rules, and oversight provided by Congress, the Executive Branch, and, as appropriate, the courts. That system of accountability ensures the privacy and civil liberties of U.S. persons.

On a daily basis, NSA/CSS provides insight into hostile plans and intentions so that our customers and partners can counter threats across the globe. Our military and its partners rely on NSA/CSS' accomplishments and products to achieve tactical and operational success. Our products are part of the fight, as essential to military operations as food, fuel, and ammunition.

Our requirements include a wide range of SIGINT missions. One of our most important SIGINT missions is counter-terrorism: discovering terrorists' plans, intentions, communications,

and locations to disrupt and defeat their attacks. As a Combat Support Agency, NSA/CSS directly supports the military with information to perform its missions and force protection, indications and warnings, and over watch support to keep our troops out of harm's way. Our work also helps the United States and its allies to capture bomb makers, spot illicit funds transfers, and explain to other nations how terrorists hope to transit their territory. We also work to identify potential threats to U.S. citizens, military personnel, and embassies around the world. In addition, we devote considerable resources to the international campaign to halt the spread of weapons of mass destruction. Tracking, reporting, and sharing data to keep nuclear, biological, and chemical weapons out of the wrong hands helps to keep the nation safe. We also assist the efforts of the Department of Homeland Security to protect America's critical infrastructure from cyberattacks. Finally, we support U.S. Cyber Command, which I also lead, and will continue to help the Command develop the capability and capacity to accomplish its vital missions.

As you well know, the threat environment – both in cyberspace and in the physical world – is constantly evolving, and we must keep pace in order to maintain our advantage. The nation's networks, communications, and data are increasingly at risk from diverse and persistent threats. These include rogue states, organized criminal enterprises, and terrorists who are showing a willingness and aptitude to employ sophisticated capabilities against us, our allies, and indeed anyone whom they perceive as a threat or a lucrative target. Various self-proclaimed cyber activists also cloud the threat picture. In addition, certain states are disposed to conduct cyber coercion against their neighbors and rivals, and to fund campaigns of cyber exploitation against us and our allies. The targets of their efforts extend well beyond government into privately owned businesses and personally identifiable information, putting the privacy and data of all Americans at risk. And terrorists' tactics, techniques, and procedures continue to evolve. Those

who would seek to harm us use the same Internet, mobile communications devices, and social media platforms that we use. As terrorists become more savvy about protecting their communications, we must keep pace in order to protect the nation and our allies.

NSA/CSS will continue to rise to these challenges. As an enterprise we have had to reinvent ourselves more than once in our history. The use of intelligence to protect our Nation dates back to the United States' very origins during the Revolutionary War. NSA's predecessors, working with their World War II partners, found German U-boats by solving Enigma machine messages. They also helped turn the tide of the war in the Pacific at Midway by cracking Japanese codes. Today, the men and women of NSA fight terrorists around the globe. During the last century, we collected and exploited Nazi and Japanese communications. Today, we target the communications of terrorist organizations who mean to do us harm, helping to uncover and thwart their efforts to communicate with sleeper cells around the world or recruit foreign fighters to their cause. The means of communications have changed, but the requirement to maintain our ability to collect and exploit the communications of hostile foreign actors remains constant. When the Information Revolution transformed communications, NSA/CSS helped lead the way toward information assurance and pioneered intelligence in cyberspace, while enabling military and counterterrorism operations in real time – in full compliance with the Constitution and the law.

Every NSA/CSS employee takes an oath to "preserve, protect, and defend" our Constitution, and the civil liberties and privacy of our citizens that the Constitution guarantees. We just repeated this oath across our workforce on 9/11. Security and privacy are not trade-offs to be balanced but complementary imperatives and NSA supports both.

The complex issues before us today represent an opportunity to write yet another chapter in the Agency's rich tradition of service. NSA/CSS plays an indispensable role in enabling our leaders to keep the peace and secure the nation. Our value lies in facilitating positive outcomes for the nation and our allies, and we have delivered this well for over 60 years. Our unique capabilities are more in demand and more important to America's security than ever. We are rightfully proud of what we have accomplished and what we continue to accomplish, and we all must strive to ensure that the American people take pride in NSA/CSS.

Mr. Chairman. Madam Vice Chairman, and Members of the Committee, thank you again for the opportunity to be here with you today; I look forward to your questions.

Chairman BURR. Admiral Rogers, thank you.

Again, for Members, we'll go directly to five-minute rounds based upon seniority.

Admiral, cyber threats continue to grow, both for the public and the private sector. NSA faces stiff competition from the private sector at recruiting those individuals with the skills that are needed. What can you offer at NSA that Silicon Valley can't offer?

Admiral ROGERS. I think the difference for us is that, as you have acknowledged, Chairman, we're competing for much of the same workforce. The advantage that we have in my mind is not unique to the cyber mission. I've experienced this as a uniformed individual for the last 34 years. It's the power of mission and the sense of serving something bigger than yourself. That ultimately is the edge that we have. That's not something you can easily replicate on the outside. It enables us to attract cutting-edge technology, incredibly motivated and capable men and women, even in the face of the fact that they could earn a tremendously greater amount of money working on the outside. But it's that sense of mission, it's that sense of purpose, it's that ethos of culture and compliance, if you will, that I think is our greatest advantage.

Chairman BURR. Admiral, NSA plays a significant role in counterterrorism efforts, discovering terrorist plans, intentions, communications, and locations, to disrupt or to defeat their attack. Obviously, we can't go into great detail here, but to what extent can you discuss it, and please elaborate on what NSA is doing to combat terrorism and, more specifically, please elaborate on what NSA's doing to combat terrorism and, more specifically, something that every American's focused on, and that's ISIL?

Admiral ROGERS. Without going into the details of how we do this, we broadly use our ability to work communications in the foreign space to generate insights as to what ISIL and other groups are doing, largely through our cyber and our signals intelligence expertise.

The challenge I would argue in the counterterrorism mission set for us, whether it's ISIL—I've seen the same thing in Al-Qaeda and Al-Qaeda in the Arabian Peninsula, for example—I've seen more changes in their behavior in the last two years probably than any other target. They actively reference some of the compromises and media leaks of the last couple of years, and we know that they have achieved a level of insight as to what we do, how we do it, and the capabilities we have that, quite frankly, they didn't have in the past.

As a result of that, quite frankly, it has become harder, more difficult, to achieve insights as to what they are doing, combined with, in fairness, the broader changes in technology we're seeing—encryption, use of apps that offer end-to-end encryption, more complicated attempts to hide in the broader set of noise, if you will, that's out there.

The positive side, though, to me is in the end it's not technology; it's about the motivated men and women of NSA. That's our edge. I always remind them, the nature of our profession is that we tend to gain advantage and lose advantage over time, because technology and the opponent's behavior always change.

Chairman BURR. Admiral, why should the American people care whether you're successful or not?

Admiral ROGERS. Because the insights that NSA is able to generate directly help to ensure the security of every citizen of this Nation, as well as those of allies and friends. I will not for one minute pretend that we are a perfect organization, but I am very proud of our mission set, the way we do it. And quite frankly, the only reason I'm still doing this is because I think the mission that NSA does is incredibly important to the Nation and our allies.

Chairman BURR. What's your greatest resource challenge right now?

Admiral ROGERS. Requirements far exceeding resources, whether it's—if you look at the growth in cyber challenges, you look at the proliferation of communications technology, trying to stay on top of this with a workforce that has not grown.

We're in our—fiscal year 2016, which we will start on October the 1st, we'll see how the budget comes out, but we project this will be the fifth straight year of a declining budget. So one of my challenges as a leader is how do we continue to generate the insights the Nation is counting on even as the resources that we use to generate those insights continue to decline.

Chairman BURR. Thank you, Admiral.

I'll turn to the Vice Chairman.

Vice Chairman FEINSTEIN. Thanks very much, Mr. Chairman. I'm going to try to get through three questions in five minutes.

Let's go, if I might, Admiral, to the USA Freedom Act. How long did it take one of your analysts to do a query under the old bulk collection system and how long does it take to do a query under the new system at the telecom companies?

Admiral ROGERS. Now, if I could, I assume by asking how long it takes to conduct a query that includes both getting the court's approval, the analysis that goes into deciding that we need to query the data. Under the old system there were several different—we had emergency authorities, for example, that I could use, which were the very quickest. Under those authorities, generally, we could do the analysis, the team could make a case to me as to why I needed to use those emergency authorities when I believed that there wasn't sufficient time to get to the court.

On those handful of occasions in which I have done that, I had to notify the Attorney General in writing, I had to notify the FISA Court in writing as to what I did and why I did it, and what the basis of my determination was. In each case, the times that I have done it to date were all driven by the fact that we were getting ready to pursue tactical action somewhere in the world that I was afraid was going to precipitate a reaction from ISIL and other groups and as a result I authorized access to the data and then informed the court and the Attorney General.

That process, probably all the analysis, them briefing me, me approving it, them going in and looking at the data, probably something less than 24 hours if you count everything.

The average under the old system, not using that emergency basis, was something—I think the fastest we ever did the entire process was something on the order of two days using the normal processes. The average was closer to four to six.

Vice Chairman FEINSTEIN. Well now, are you saying you have to use the emergency more often?

Admiral ROGERS. No.

Vice Chairman FEINSTEIN. You said five or six instances.

Admiral ROGERS. No. We queried the data multiple times through a court approval. There were a handful of times that I——

Vice Chairman FEINSTEIN. Well, you're saying it's faster now?

Admiral ROGERS. No. That is under the old system. You asked me to compare old versus new. I'm just trying to give you a framework for under the old system.

Under the new system, because it's not implemented I can't tell you right now. Remember, we're in the process of transitioning. The transition must be complete by the end of November 28th.

Vice Chairman FEINSTEIN. So you haven't done any?

Admiral ROGERS. We have not completed the process yet. That's why the legislation we had asked—this is going to take some number of months to work with the providers, to make the technical changes on the provider side.

Vice Chairman FEINSTEIN. Got it.

Second subject. Sunday's "New York Times" reported that our country will ask the Chinese to embrace the United Nations Code of Conduct on Principles for Cyberspace that no state should allow activity, quote, "that intentionally damages critical infrastructure and otherwise impairs the use and operation of critical infrastructure to provide services to the public." From your perspective, would a cyber arms control agreement along these lines be valuable? Would it be enforceable?

Admiral ROGERS. First, that's a broad policy question. In terms of the input, my opinion, the devil is always in the details. I'd want to understand the specifics of exactly what we are talking about.

Vice Chairman FEINSTEIN. That's a good duck. It just doesn't quack.

Admiral ROGERS. I apologize, but there are so many variables in this.

Vice Chairman FEINSTEIN. Let's move on. I wanted to ask you about the use of encrypted communications by terrorists and criminals. The FBI Director came before us, as you know, and gave us very stark testimony about going dark and how big the problem was. Do you believe that the increased use of this kind of encryption and apps, as you pointed out, poses a national security threat?

Admiral ROGERS. Yes, ma'am. I am concerned that the direction we're going is effectively—if we make no changes, represents a significant challenge for us in terms of our ability to generate insights that the Nation is counting on.

Vice Chairman FEINSTEIN. Can we make changes?

Admiral ROGERS. I'm the first to acknowledge it's a complex issue. I'd make a couple points. First, I don't think you want the government deciding, hey, what the right answer is here. We have got to collectively get together between the private sector, government, industry, policy, the technical side and sit down and figure out how we're going to work our way through this, because I'm the first to acknowledge this is an incredibly complex topic and there are no simple and easy answers here.

I believe that, like anything, hey, if we put our mind to it, we can ultimately come up with a solution that is acceptable to a majority. It likely won't be perfect and I'm the first to acknowledge you don't want me or an intelligence organization making those kinds of decisions, you don't want us able to unilaterally do that. I'm the first to acknowledge that.

Vice Chairman FEINSTEIN. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Senator Coats.

Senator COATS. Thank you for your service. I appreciate it. To follow up on Senator Feinstein's questions, if I heard you right, under the old system, given the procedures that you go through, if it's an emergency you can get clearance in less than 24 hours?

Admiral ROGERS. Under the previous framework, I as the Director of NSA was delegated the authority in emergency situations to authorize access to the data. I then had to go to the court and to the Attorney General and put in writing why I did it, what I did, and what the basis of that decision was.

Senator COATS. What if it's imminent? What if you get a call that a plane took off in Boston, turned south toward New York when it was scheduled to go to Montreal, and you said that will arrive in New York air space in 15 minutes? What happens?

Admiral ROGERS. That's one of the reasons for that emergency authority, so that I have the authority under the current system. Now, as we transition to the new law, which again we have to have permanently in place by November the 29th, I have lost that authority. It has now been raised to the Attorney General. So I will have to approach the Attorney General for why she, in this case she, needs to authorize emergency access.

Senator COATS. So we're adding time to the process?

Admiral ROGERS. It's probably going to be longer, I suspect we're going to find out.

Senator COATS. And based on my question and your answer, something that imminent probably can't be addressed in time to put up the defenses?

Admiral ROGERS. Not in minutes. I doubt we could do it in minutes.

Senator COATS. You stated in your statement here that NSA works daily to protect privacy and civil liberties. We've seen breaches of tens of millions of Federal employees' records. We've seen breaches of well over 50 million of a major insurance company in my State. We've seen breaches of everything from retail stores to you name it.

Obviously, those occur partly because those entities did not have the procedures in place to block that. NSA does. Yet you're criticized, your agency's been criticized, for being too loose on privacy, can't trust you. But all the information—and you're collecting phone numbers and names of individuals you don't know. And the breaches are occurring with all kinds of information of when you were born and what your Social Security number is and what your bank account number is and everything else.

So give me again for the record just what kind of things NSA went through and continues to go through that protects privacy and civil liberties, and if you can an explanation of why NSA is

deemed untrustworthy holding information, and yet we rely on institutions that leak the stuff by the tens of millions?

Admiral ROGERS. If I could, let me answer the second part first. It's one of the great challenges for me as a leader and I would argue for us as a Nation. Increasingly, we find ourselves as a society distrustful of government, writ large, and in the aftermath of media leaks, NSA in broad terms.

I think that's both a part of this broader environment that we currently live in right now—you see it in the fact that we're unable to achieve—you live this every day in your political lives—we're unable to achieve political consensus on difficult issues that face the Nation. We have strong opinions and yet we can't seem to come to a consensus about how we move forward on many things.

What is happening to NSA is a part of that broader context. So we find ourselves in a position where we acknowledge we must follow the law, we acknowledge we must operate within a legal framework and the set of authorities and policies. We do not indiscriminately collect. Everything we do is driven by the law and a set of priorities as to exactly what we do and what we focus on. Those priorities designed to generate insights to help defend our Nation, not to violate people's privacy.

But in the world we're living in now, that seems to get lost in the ether in many ways, part of the challenge being as a classified organization, if you will, the how we do what we do, because I can't go into great details about, well, this is exactly why you should feel comfortable, let me walk you through all the things we have done that you have no clue about but you should feel very comfortable with as a citizen or an ally about what we've been able to forestall.

In terms of what we put in place to attempt to ensure the privacy and civil liberties of our society, you look at the legal framework that collectively was created for the call data records, USA Freedom Act. You look at what we have done in terms of complying with court orders. You look at what we have done in terms of NSA has had three major outside reviews—702, the Section 215, the call data records, of our collection in general. Every one of those reviews has come back with the same conclusion: You can argue that the law is good or bad, but NSA is fully compliant with the law.

NSA has a systematic system in place designed to ensure oversight and protection of the data we collect. We ensure that not everyone in our workforce can just access any one that we collect. The call data records, for example, Section 215, out of an organization, as I told you in my opening statement that's close to 40,000, we have limited access to that data to 30, approximately 30 people by design. We want—we understand the sensitivity and the importance of the data that we collect, and we need to ensure that we can tell you as our oversight, as well as the broader citizens we defend, that we are not arbitrarily misusing this data, that we are not opening it up to just anyone in our workforce who wants to look at it.

We take those duties and those responsibilities very seriously, and each one of the three major independent reviews we've had in the last 18 months have come to the exact same conclusion in that regard.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

Thank you, Admiral, for your professionalism.

Let's see if we can do the first question on bulk collection, this matter of collecting all the millions of phone records on law-abiding people, with just a yes or no answer, because I know Senator Feinstein got into some of the questions with respect to implementation. I have heard you comment on this, but I'd like to see if we could do this on the record. Do you expect that ending bulk collection is going to significantly reduce your operational capabilities?

Admiral ROGERS. Yes.

Senator WYDEN. In what way?

Admiral ROGERS. Right now, bulk collection gives us the ability to generate insights—we call it discovery—gives us the ability to generate insights as to what's going on out there. I'd also encourage the panel, as well as the Committee, as well as the Nation, to review the National Academy of Sciences review, in which they were specifically asked: Is there an alternative to bulk collection? Is there software or other things that we could develop that could potentially replace NSA's current approach to bulk collection? That independent, impartial, scientifically founded body came back and said: No, under the current structure there is no real replacement and that bulk collection as used by NSA generates value.

Senator WYDEN. But, as you know, the President's Advisory Committee disagreed with you. They had an independent group appointed and they said—and I believe it's at page 104 of their testimony—that there was no value to bulk collection that could not be obtained through conventional means, and it's specifically cited.

Let me ask you about encryption, because in my view this is a problem largely created by your predecessors, General Hayden and General Alexander specifically. I believe they overreached with bulk collection. That undermined the confidence of consumers and the companies responded because they were concerned about the status of their products with strong encryption.

So at that point I began to be pretty concerned because it looked like the government's position was companies would be required to build weaknesses into their products. Now the discussion has shifted to whether there should be the availability of encryption keys to access these products. Now, I don't want to go into anything classified or matters relating to Executive Branch discussions. But let me ask you about a policy matter. As a general matter, is it correct that any time there are copies of an encryption key and they exist in multiple places, that also creates more opportunities for malicious actors or foreign hackers to get access to the keys?

Admiral ROGERS. Again, it depends on the circumstances. But if you want to paint it very broadly like that for a yes and no, then I would probably say yes.

Senator WYDEN. Okay. I'll quit while I'm ahead.

What concerns me, Admiral, seriously is that as this question of access to encryption keys is pursued—and I think that's where we move, as I indicated to you in our conversation, from the original position, which looked like companies would have to build weaknesses into their products, which I think is a staggering development, it seems now it has shifted with Ms. Yates's comments and others to this question of the availability of keys.

You've just told me as a general proposition when there are multiple keys—and there will be multiple keys—that creates more opportunities for malicious actors or foreign hackers. And to me, the good guys are not going to be the only people with the keys. There are going to be people who do not wish this country well. That's going to provide more opportunities for the kinds of hacks and the kinds of damaging conduct by malicious actors that I think makes your job harder.

I think you're doing a good job. I think you've been straight with the Congress and certainly with me. But that's what concerns me about access to malicious keys, and I appreciate your answer on that.

Go take a look at page 104 of the President's Advisory Committee, because on this question of operational capabilities, not only do we not have any cases that indicated that there was a compromise of the abilities of our intelligence community, it was the unanimous finding of the President's experts. That page will give it to you.

Thank you, Mr. Chairman.

Chairman BURR. Senator Rubio.

Senator RUBIO. Thank you.

Thank you, Admiral, for being here. As you're aware, the Chinese president, the leader of the Chinese Communist Party, Xi Jing Ping, is going to be in the White House this week and to receive the full honors of a state visit. But our relationship with China is not at a good place at this moment. They've breached the U.S. Government databases, they continue cyber attacks against other elements of our government. Over the last 20 years we've witnessed the single largest transfer of wealth in the history of the world as Chinese companies, backed by the Chinese government, have stolen proprietary data and U.S. State secrets, and now, of course, the personal data of at least 25 million Americans, if not more.

One of the things I've advocated is a three-step process. I think we should be expelling known Chinese spies that are operating in the U.S. as retaliation for these cyber attacks. I think we should be disconnecting all sensitive databases from the internet and ensure that our agencies that are responsible for protecting government databases are doing their job. And I think we need to make clear that we're going to respond in kind to deter adversaries like China who will continue to attack us.

I guess my question begins by asking you: Would you agree that a public discussion on an offensive cyber capability would be an effective deterrent?

Admiral ROGERS. I think we as a Nation need to have a very public discussion about how do we achieve this idea of deterrence, because if we don't change the current dynamic we are not in a good place. We have got to fundamentally change the dynamic we're dealing with now.

Senator RUBIO. As the Director of NSA and as Commander of U.S. Cyber Command, have you provided advice to the President—I'm not asking what the advice is, but have you provided advice to the President or the White House on ways to defend against cyber attacks, cyber deterrent strategy, and appropriate measures for us to respond to such attacks?

Admiral ROGERS. Yes.

Senator RUBIO. I understand that you're not charged with creating policy, but has the White House sought your opinions on policies relating to these matters, specifically on a more effective cyber deterrent and best practices for securing U.S. Government systems?

Admiral ROGERS. Yes. I'm very happy in the process in the sense that, hey, I'm just one perspective. I certainly understand that. But I've certainly had the opportunity to communicate my views as to what I think we need to do.

Senator RUBIO. I guess my last question is going back to the points that I've raised about expelling Chinese spies operating in the U.S. as retaliation and also disconnecting the sensitive databases from the internet. Are these measures that you think are worthy of exploration? Would they have any sort of deterrent effect or be part of the broader public discussion about this issue?

Admiral ROGERS. Certainly in my experience one of the things we've found and one of the challenges, particularly for Cyber Command, my other hat where I deal with penetrations in the Department of Defense, one of the things that we have come to understand is you need to minimize your exposure with what we call public-interfacing web sites, connectivity with the internet.

The flip side, though, is that there is a requirement in many instances to ensure information flow from the internet in the system. And so the idea that you're going to be able to do some of these things with no internet connectivity, again it depends on the situation. It can be problematic if you expect data to flow back and forth.

Senator RUBIO. I just have one last question. I apologize. It's kind of a matter of doctrine, more or less. Our doctrine, the doctrine of most nations, if not all on Earth, is that there is a difference between intelligence gathering on governments and intelligence gathering on private entities. Clearly, multiple nations, if not all around the world, have some sort of intelligence gathering capability and it's targeted primarily at the governments and government actors in other nations, especially those they have an adversarial position with.

Is it fair to say that for the Chinese there is no such distinction, that for them the notion of intelligence gathering, they view commercial intelligence gathering and governmental intelligence gathering as all part of their foreign policy and intelligence gathering capability? They don't have that distinction that we have or other nations have; is that an accurate assessment?

Admiral ROGERS. They clearly don't have the same line in the sand, if you will, in that regard. I watch some of my counterparts there do things that under our system I could never do.

Senator RUBIO. Exactly. So the point I'm trying to drive at, because many Americans are not perhaps fully aware of this, is that the Chinese government actively encourages as part of their national policy the stealing of commercial secrets of American companies for purposes of building up their own capability, and this is directed by government. This is not like a Chinese company hacking an American company. This is directed, influenced, and funded by the network government itself.

Admiral ROGERS. Yes.

Senator RUBIO. Thank you so much for your service.

Chairman BURR. Senator Warner.

Senator WARNER. Thank you, Admiral Rogers, for your service.

Let me just add an editorial comment here to the Chair and the Vice Chair. My hope would be, in light of the testimony of Admiral Rogers, that we could urge the respective leaders in both parties to bring that information-sharing bill that's passed out of our Committee back to the floor. I think we do a great disservice to our country if we don't act on that legislation as quickly as possible.

Chairman BURR. The Vice Chair and I can assure all the Members we are working aggressively to get that back up, and my hope is that Members will have an opportunity, not only to debate it, but to amend it if need be in the month of October.

Senator WARNER. Thank you, Mr. Chairman.

Admiral Rogers, I'm going to spend a couple moments on the OPM breach. Obviously, 22 million-plus individuals, now we're understanding 5.6 million fingerprints. We dug into that and I know you can't comment too much, but that we found—and Senator Collins and I are working on legislation that says as we look at the responsibilities of DHS to try to protect the dot-gov regime, they don't have the same kind of abilities and responsibilities that you have to defend the dot-mil regime when it comes to cyber hygiene. DHS actually has an ability to recommend, but not actually enforce.

Recognizing this may be more asking for your editorial view here, do you want to make a comment on that?

Admiral ROGERS. First, I would argue those authorities to defend DOD networks really reside operationally more in my U.S. Cyber Command role. But it's fair to say—and again, it's all I guess part of the cultures that spawn us—in the Department of Defense our culture is you're always focused on generating actionable outcomes. You're focused on empowering individuals and clearly identifying responsibility and authority and then holding people accountable.

I think what we want to get to in the dot-gov domain is something quite similar over time. I think it's fair to say that we're not there right now.

Senator WARNER. We have, Senator Collins and I, have legislation that would give DHS similar type authorities, as well as that in effect chain of command. There still seems to be some lack of clarity about who's in charge. We hear constantly, even including OPM, that DHS made recommendations about cyber hygiene that were not implemented by OPM and a variety of other dot-gov regimes. That to me seems not good process going forward.

Can you speak to, within this setting, what responsibility you have in protecting cyber—in protecting sensitive but unclassified data on the dot-gov side of the house?

Admiral ROGERS. I do not have immediate responsibility, in the sense that the structure is that I at NSA work through DHS to provide support when it's requested. I am not in those networks. I am not monitoring those networks.

Senator WARNER. And post-OPM, has DHS requested your assistance?

Admiral ROGERS. Yes.

Senator WARNER. Again, this is an area that I believe would be addressed as well, hopefully with at least an amendment to the information-sharing bill, something I know Senator Collins and I, and I think most of our other colleagues share, we need to give DHS those same tools.

Let me switch over to an area where Senator Rubio was. I concur with him that, while we've not formally identified the source of the OPM breach, there is obviously speculation amongst Members and the press. My comment as well is that we do need a deterrence as part of our overall national strategy.

I'd like you to make any comment you might have on—again, we're playing on different standards. The Chinese in July passed legislation that required all of their information systems and companies that do business in China to have systems that were secure and controllable in terms of access by the Chinese authorities, which not only precludes any of the kind of encryption tools that American domestic companies are looking at, and again I think raise huge concerns—I agree fully with Senator Wyden, but I do think there are concerns to be raised. But also, this "secure and controllable language," wouldn't that be in effect an open ability for Chinese authorities to potentially get into those companies' databases for intellectual property theft and other activities?

Admiral ROGERS. The Chinese have a fundamentally different construct than we do. They believe in essence that access to the content of communications and data is a sovereign right. We reject that notion. It leads to some of the things that we have seen them do. It's why we have very publicly discussed this with our Chinese counterparts, because in the end we want to get to a place where we can both work together. But the current approach, where we are so fundamentally apart, we've been very up front that this is just not acceptable. We can't sustain a long-term relationship, the kind of relationship we want, if this is the approach, that the privacy of individuals, the access to intellectual property, is just viewed as something the state can do at the time and place of its choosing. It goes totally against our framework.

Senator WARNER. I hope our President will continue to raise this.

Again, Mr. Chairman, my hope is that so many of the businesses that we saw meeting with President Xi the other day in Seattle, I hope they will not default to a lower standard in their rush to try to access the Chinese market. Thank you, Mr. Chairman.

Chairman BURR. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Admiral Rogers, let me add my thanks to those of the Committee for your dedicated service.

You mentioned, in response to a question from Senator Coats, that only 30 NSA employees had access to the metadata, were authorized to query the database. Am I correct in assuming that those 30 employees were well vetted, they were trained, and that they would be held responsible if there were any misuse of the information?

Admiral ROGERS. Yes, ma'am.

Senator COLLINS. Has there ever been any misuse of the information that you're aware of?

Admiral ROGERS. No, ma'am. The only thing I would highlight in terms of oversight and compliance, for example, for those 30 individuals, we monitor every keystroke they use in trying to access the data. We don't do that for every one of our tens of thousands of other employees. We do it in this regard because we realize the sensitivity of the data.

Senator COLLINS. I think that's an excellent point that should have been reassuring to me. It's very ironic that the USA Freedom Act was passed under the guise of increasing privacy protections for the American people when there are 1,400 telcom companies, 160 wireless carriers. Not that you're necessarily going to have to deal with all of those, but isn't it likely that far more than 30 people will now be involved in this process?

Admiral ROGERS. Yes, I would expect that to be the case.

Senator COLLINS. And given that those companies market and sell a lot of this information, aren't the privacy implications far greater with this new system than under the careful system that you described, with only 30 people authorized?

Admiral ROGERS. I would respectfully submit that's for others to decide.

Senator COLLINS. Well, I think from your—I understand why you're saying that, but I think if one just looks at the numbers the case becomes very evident.

In the USA Freedom Act, there's no requirement for the telcom companies to retain the call detail data, and by that I'm not talking about content. I'm talking about call detail data. That's another misconception that some people have. There's no requirement that that data be held for any particular period of time. Companies hold it for their own business records purpose. Is that a concern to you?

Admiral ROGERS. Based on our initial interactions with the providers as we move from the old structure to the new structure where the providers hold the data, in talking to them there's a pretty wide range. We're right now dealing with the three largest, who really have been the focus of the previous structure. We will bring additional on line, as you have indicated. Among those three that we're starting with initially, a pretty wide range of how long they opt to retain data and for what purposes. Again, under the construct that's their choice. We'll have to work our way through this.

One of the things I have always promised in the discussion that led as part of the legislation was, once we get into this new structure, what I promise will be honest and direct feedback on how this is working. Is it effective, is it not effective? What kind of time duration is it taking us? What have been the operational impacts? I have promised I will bring that back once we get some actual experience.

Senator COLLINS. We appreciate that.

Let me turn to a different issue and that is the protection of our critical infrastructure from cyber threats and cyber intrusions, which is an issue that's long been of huge concern to me. The Department of Homeland Security has identified more than 60 entities in our critical infrastructure report damage caused by a single cyber incident could reasonably result in $50 billion in economic

damages or 2,500 immediate deaths or a severe degradation of our national defense.

Your testimony, your written testimony, talks a little bit about this issue. Your predecessor, General Alexander, previously has said that our Nation's preparedness when it comes to protecting against a cyber attack against our critical infrastructure is about a three on a scale of one to ten. Where do you think that we are on that scale?

Admiral ROGERS. It varies by sector, but on average I'd probably say right now, again depending on the sector, we're probably a five or a six. That's not where we need to be, clearly.

Senator COLLINS. So there's still a severe problem in this area that makes us very vulnerable as a Nation?

Admiral ROGERS. Yes, ma'am.

Senator COLLINS. Thank you.

Chairman BURR. Senator King.

Senator KING. Admiral Rogers, greetings.

Would a shutdown of the Federal Government next week compromise national security?

Admiral ROGERS. Yes. And if I could, just to go beyond that. In the last five days or so, as we now are publicly talking about this possibility, watching the reaction of the workforce at NSA and U.S. Cyber Command, who are going "Again?," who could easily get jobs on the outside and earn significantly more amounts of money, this instability, this message to the workforce that—this is probably a pejorative, but—you are a secondary consideration in a much larger game, if you will, that drives——

Senator KING. No, no. It's a smaller game, Admiral.

Admiral ROGERS. Smaller game. It just drives the workforce, to the point where today I literally was talking to the leadership about, we need to sit down and figure out how we're going to keep these men and women. If their attitude increases——

Senator KING. Keeping these talented men and women is hard enough to begin with because of higher salaries outside. There's a survey I commend to your attention, I'll submit for the record, done late last year of national security professionals across the government. One of the fascinating results is that U.S. political dysfunction they ranked as a higher threat to national security than a nuclear-armed Iran, Vladimir Putin, China's military buildup, or North Korea. The only thing above political dysfunction was Islamic extremism. So that is shocking.

[The material referred to follows:]

Defense One

Political Dysfunction Is a Worse Threat Than Putin, Say National Security Workers

By Kevin Baron

November 18, 2014

The Obama administration has no strategy for ISIS, the Pentagon is not leaving enough troops to protect Afghanistan and Congress isn't qualified to keep watch over the military and intelligence services, according to survey of federal workers and troops at the Pentagon, and other national security agencies.

It's a grim report card for Washington, where U.S. leaders have struggled to respond decisively to conflicts from Russia to Ramadi while political leaders have left the national security workforce guessing for a budget and more direction from their leaders.

In a survey of national security professionals in government, Islamic extremism ranks No. 1 among global threats, but the No. 2 choice is a tie between cyber attacks and U.S. political dysfunction.

In fact, political dysfunction ranks ahead of "international terrorism," "a nuclear armed Iran," and Russia, China and North Korea, in the minds of these respondents.

The list of mistrust in government leadership is long. Seventy-three percent think Obama does not have "a clear national security strategy." Not just an ISIS strategy -- but a strategy for all national security. Only 26 percent approve of Defense Secretary Chuck Hagel. And 20 percent of federal workers and troops surveyed think members of Congress are qualified to perform their oversight duties for national security.

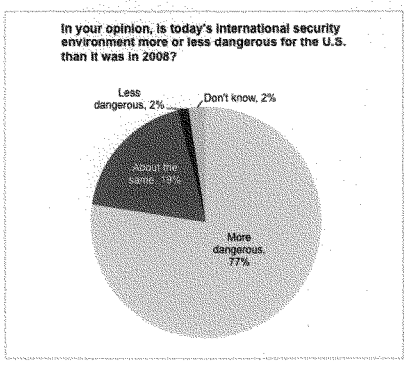
If you think DOD and similar workers are inherent war hawks, look more closely.

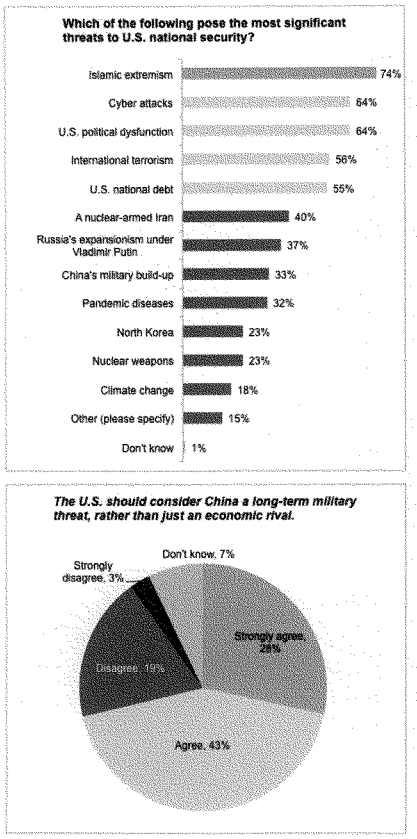
Half of those surveyed think the U.S. relies too much on the military to achieve foreign policy goals. Short of a direct attack on the homeland or NATO, fewer than half want to use force to fight -- not if Iran gets nuclear capability, not to stabilize a Middle East ally, not even to stop genocide. Even if the Taliban threaten to regain control of Afghanistan, barely one quarter of respondents said they'd support military intervention again.

And Iraq? Was the Iraq War worth its cost? Only 24 percent said yes.

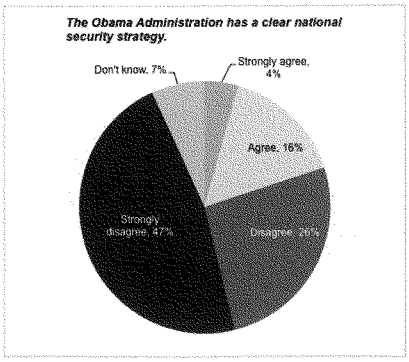
Defense One and Government Business Council, divisions of Atlantic Media's Government Executive Media Group, sent an email-based survey to a random sample of *Government Executive*, *Nextgov*, and *Defense One* subscribers. Of those, 427 respondents from the Departments of Defense, Homeland Security and State completed the survey, including those at the GS/GM-11 to 15 grade levels, active duty military personnel, and members of the Senior Executive Service; 55 percent of respondents are GS/GM-13 and above or the military equivalent; 77 percent are DOD civilians; 7 percent are active duty military personnel. The results have been weighted by service branch and agency. The margin of error is +/- 4.74 percent.

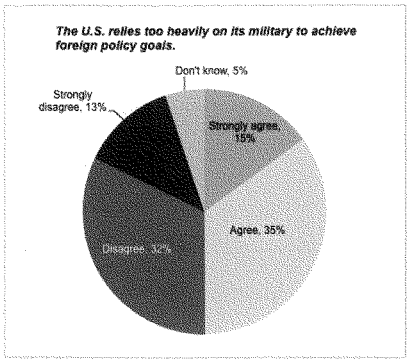
The Current Threat Environment

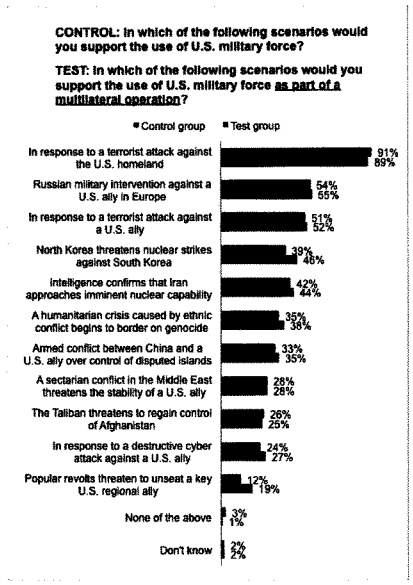




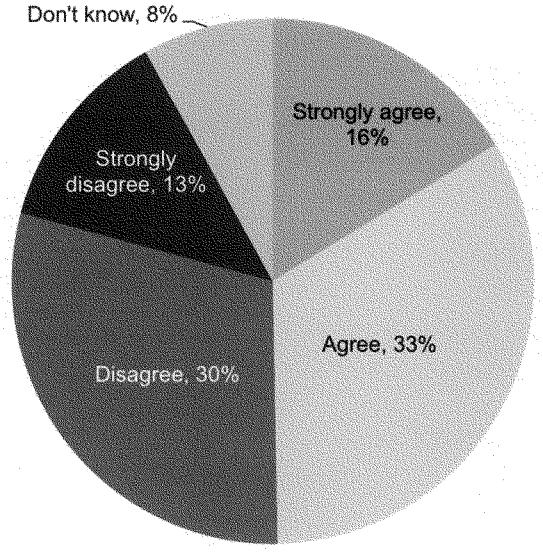
U.S. National Security Strategy


The Obama Administration has a clear national security strategy.
Don't know, 7%
Strongly agree, 4%
Agree, 16%
Strongly disagree, 47%
Disagree, 26%

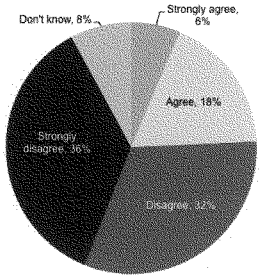

The U.S. relies too heavily on its military to achieve foreign policy goals.
Don't know, 5%
Strongly disagree, 13%
Strongly agree, 15%
Agree, 35%
Disagree, 32%

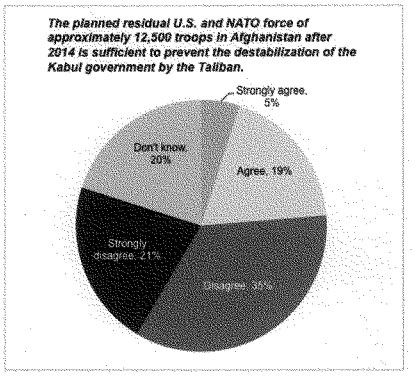

CONTROL: In which of the following scenarios would you support the use of U.S. military force?
TEST: In which of the following scenarios would you support the use of U.S. military force as part of a multilateral operation?
Control group
Test group
In response to a terrorist attack against the U.S. homeland
91%
89%
Russian military intervention against a U.S. ally in Europe
54%
55%
In response to a terrorist attack against a U.S. ally
51%
52%
North Korea threatens nuclear strikes against South Korea
39%
46%
Intelligence confirms that Iran approaches imminent nuclear capability
42%
44%
A humanitarian crisis caused by ethnic conflict begins to border on genocide
35%
36%
Armed conflict between China and a U.S. ally over control of disputed islands
33%
35%
A sectarian conflict in the Middle East threatens the stability of a U.S. ally
28%
28%
The Taliban threatens to regain control of Afghanistan
26%
25%
In response to a destructive cyber attack against a U.S. ally
24%
27%
Popular revolts threaten to unseat a key U.S. regional ally
12%
19%
None of the above
3%
1%
Don't know
2%
2%

The U.S. should have intervened in Syria following the Syrian government's use of chemical weapons in August 2013.

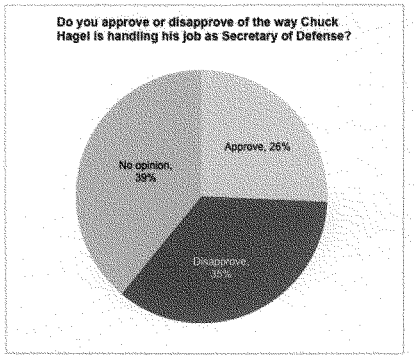


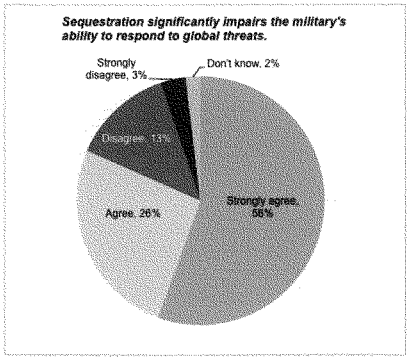
The U.S. military intervention in Iraq from 2003-2011 was worth its cost.

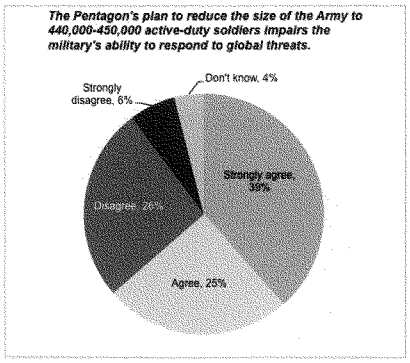


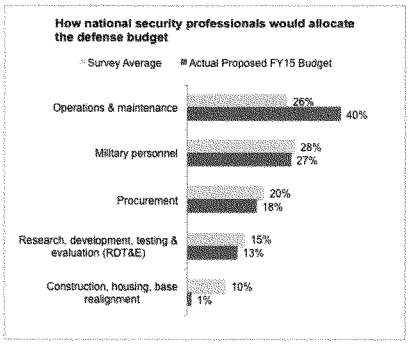


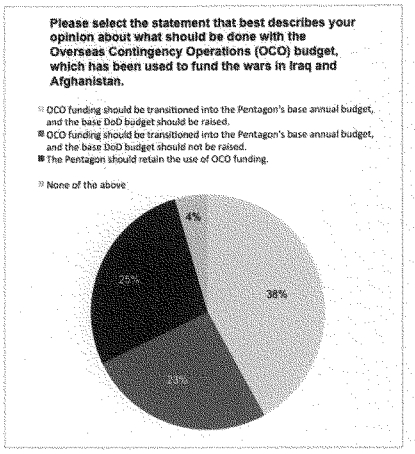
Spotlight on the Pentagon

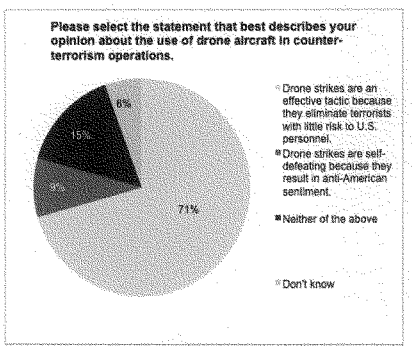



Sequestration significantly impairs the military's ability to respond to global threats.
Strongly disagree, 3%
Don't know, 2%
Disagree, 13%
Strongly agree, 56%
Agree, 26%


The Pentagon's plan to reduce the size of the Army to 440,000-450,000 active-duty soldiers impairs the military's ability to respond to global threats.
Strongly disagree, 6%
Don't know, 4%
Strongly agree, 39%
Disagree, 26%
Agree, 25%

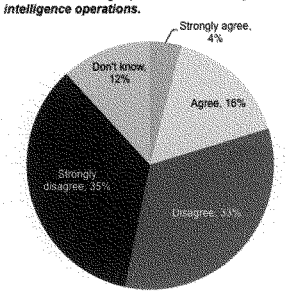

How national security professionals would allocate the defense budget
Survey Average
Actual Proposed FY15 Budget
Operations & maintenance
26%
40%
Military personnel
28%
27%
Procurement
20%
18%
Research, development, testing & evaluation (RDT&E)
15%
13%
Construction, housing, base realignment
10%
1%



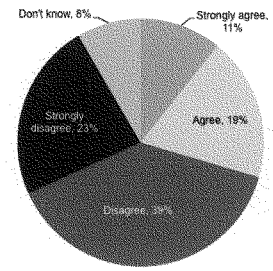


The Politics of National Security

Enough current members of Congress are qualified to exercise oversight powers over military and intelligence operations.



The White House overstepped its war powers authority when commencing military operations against the Islamic State (ISIS or ISIL).

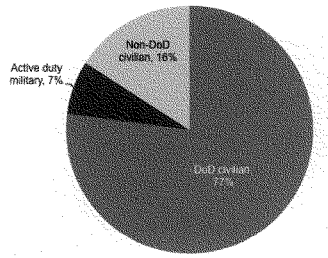


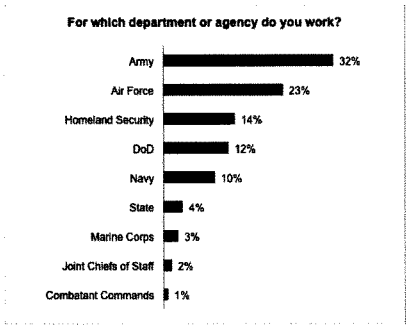
Please rank the following prospective 2016 presidential candidates in order of their national security credibility.

Candidate	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	Mean Rank
Mitt Romney	34%	20%	16%	9%	4%	4%	5%	2%	2%	5%	3.0
Jeb Bush	16%	23%	18%	14%	9%	7%	6%	3%	2%	3%	3.7
Hillary Clinton	44%	15%	7%	4%	1%	3%	2%	3%	10%	11%	3.8
Paul Ryan	11%	13%	13%	13%	19%	9%	6%	9%	4%	3%	4.6
Rick Perry	11%	13%	15%	14%	8%	11%	9%	8%	6%	6%	4.8
Chris Christie	15%	10%	12%	11%	8%	10%	15%	14%	3%	3%	4.9
Rand Paul	11%	8%	17%	13%	11%	9%	10%	12%	8%	2%	5.0
Joe Biden	11%	36%	6%	2%	3%	2%	3%	6%	13%	20%	5.1
Marco Rubio	4%	8%	13%	15%	15%	20%	10%	8%	7%	1%	5.2
Ted Cruz	8%	12%	11%	13%	9%	8%	10%	8%	11%	12%	5.6

Survey Sample Demographics

Which best describes your employment situation?





By Kevin Baron // Kevin Baron is the founding executive editor of *Defense One*. Baron has lived in Washington for 20 years, covering international affairs, the military, the Pentagon, Congress, and politics for *Foreign Policy*, *National Journal*, *Stars and Stripes*, and the *Boston Globe*, where he ran investigative projects for five years at the Washington bureau. He is a frequent on-air contributor and previously was national security/military analyst at NBC News & MSNBC. Baron cut his muckraking teeth at the Center for Public Integrity and he is twice a Polk Award winner and former vice president of the Pentagon Press Association. He earned his M.A. in media and public affairs from George Washington University, his B.A. in international studies from the University of Richmond, and studied in Paris. Raised in Florida, Baron now lives in Northern Virginia.

November 18, 2014

http://www.defenseone.com/ideas/2014/11/political-dysfunction-worse-putin-say-national-security-workers/99344/

Senator KING. Let me move on. Political dysfunction being a national security threat: Pogo: "We have met the enemy and he is us."

A couple of other questions. Deterrence. You've talked about it briefly. I want to emphasize—you testified that you were in communication with the White House and the President on this issue. I think this has got to be a high priority. Deterrence doesn't work unless people know about it, and it's got to be a strategy because right now we are in a fight. The cyber war has started and we are in the cyber war with our hands tied behind our backs. We would never build a destroyer without guns.

We've talked about this before. I think—I hope you will carry this message back, because we've got to fashion a theory of deterrence. Otherwise, we are going to lose. You cannot defend, defend, defend, defend and never punch back. And if your opponent knows you're not going to punch back, it's just not going to go anywhere.

If you can find a question in there, you're welcome to it. But I think you understand.

Admiral ROGERS. Yes, sir.

Senator KING. I hope you will take that message back. You're a very strong advocate and you're the right guy to take that message.

Another question that's been touched upon is the idea of a cyber-nonproliferation treaty. I find that a fascinating concept and I wish you would expand a bit on that, that we can establish some rules of the road in this field for our mutual protection of the various countries that are cyber capable.

Admiral ROGERS. I certainly think we can get to the idea of norms. Formal treaty, I don't know, because one of the challenges in my mind is how do we build a construct that ultimately works for both nation-states and non-state actors. One of the challenges inherent in cyber is the fact that you are dealing—unlike the nuclear world where you're dealing with a handful of actors, all nation-states, you're dealing with a much greater number of actors, many of whom, quite frankly, are not nation-states and have no interest in sustaining the status quo, so to speak. In fact, if you look at ISIL and other groups, their vision would be to tear the status quo down. They're not interested in stability.

Senator KING. I just think that this is a promising area with other nation-states. Obviously, it's not going to be the whole solution, but if there are states like Russia or China that are willing to have this discussion I think it's a profitable discussion.

Admiral ROGERS. Right.

Senator KING. Along with the idea of deterrence, because we are asymmetrically vulnerable in this war. We're the most wired country on Earth and that makes us the most vulnerable country on Earth.

Well, I appreciate your testimony and the work that you're doing. Oh, you testified a few minutes ago that you had a variety of reactions from the telecoms about retention levels. You said they were short to long. What's the shortest that you've been informed of?

Admiral ROGERS. I want to say it's something on the order of 12 to 18 months.

Senator KING. Okay, so that's on the short end. I hope you will let this Committee know if it goes below that level, because at that

point it becomes very problematic as to whether or not the data being retained will be of usefulness in a national emergency.

Admiral ROGERS. I will.

Senator KING. Thank you, Admiral.

Thank you, Mr. Chairman.

Chairman BURR. Senator Lankford.

Senator LANKFORD. Admiral, thanks for being here. Thanks for your leadership in your work. We've had multiple conversations and I appreciate what you bring to this. Answer this for me: What else can NSA do to help other agencies deal with cyber deficiencies? We've had some extremely public cyber deficiencies of the Federal Government of late. What assets can NSA bring to bear to be able to help on this? I think you end up coming in to clean up the mess as much as you end up trying to help defend. How do we get proactive on this?

Admiral ROGERS. What I'd like to do—and again, we'll be part, NSA will be part of a broader team. What I'd like to do is be proactive and get ahead of this problem set.

Senator LANKFORD. Currently the agencies have responsibility to be able to take on and make sure that their systems are all protected. There doesn't seem to be a lot of accountability in the structure. There are people advising agencies, but what can be done proactively?

Admiral ROGERS. I'd be interested, for example, in could we build a framework where someone from outside the organization is doing an independent assessment, as an example. I can within the DOD, largely under U.S. Cyber Command authority, but I also do this with NSA. I can go into any dot-mil network anywhere in our structure. I can assess it. I can test it. I can attempt to penetrate it. I don't have to give notice to the network owner, as an example. That really doesn't exist on that scale anywhere else in the government.

I'd like to see what we can do to try to, again, get ahead of the problem set, try to replicate some of the activities we're seeing from opponents ahead of time before they do it, and test our abilities.

Senator LANKFORD. Let me ask about auditing and how you do that for your own people and processes. You mentioned, for instance, on these 30 folks in the past every keystroke has been monitored. How often do you do auditing and how do you audit that? You have an incredible group of folks that serve the Nation, but obviously the accountability of the network is extremely important. We've had rogue folks in the past take information.

Admiral ROGERS. Auditing varies. As I've said, those 30 individuals, the call data record database, that's probably the area we put more external monitoring and controls in than any other part of our structure. On the other hand, in the aftermath of the media leaks, we've sat back and asked ourselves, so how could this have happened? What have we failed to do as an organization and what do we need to do to ensure it doesn't happen again?

We put a series of capabilities in place where we can monitor behavior. We put a series of capabilities in place where we look at personal behavior more, although I will tell this is another issue that often can provoke a strong reaction from the workforce, who says: So let me understand this; because of the actions of one indi-

vidual, you are now monitoring me; you're now watching my behavior in a way that you didn't necessarily do before. Do I want to work in a place like that?

We try to sit down with the workforce and walk through: here's what we do and here's why we do it. But there's a reason behind it, that each one of us as we voluntarily accept access to the information that we're given, we hold ourselves to a higher standard. We hold ourselves to a different level of accountability. That's part of the quid pro quo here if you're going to be an NSA professional, if you're going to be an NSA employee. But it is not lost on our workforce at times.

Senator LANKFORD. Let's talk about the cyber war we're dealing with internationally at this point. The biggest threats that we have, are they state actors or non-state actors at this point internationally?

Admiral ROGERS. Let me answer it this way if I could. The greatest amount of activity is still criminal-based, but when I look at from a national security perspective, I would argue at the moment the nation-state represents the greater national security challenge, if you will.

When I look at the future, there's three things—and I've said this publicly before—that concern me the most when it comes to cyber. Number one is something directed, destructive activity directed against critical infrastructure. Number two is manipulation, changes to data. At the moment, most of the activity has been theft. What if someone gets in the system and starts just manipulating, changing data, to the point where now as an operator you no longer believe what you're seeing in your system?

The third area that I think about in terms of concerns about the future, really to go to your question, is what happens when the non-state actor decides that the web now is a weapon system, not just something to recruit people, not just something to generate revenue, not just something to share their ideology?

Senator LANKFORD. So the relationship between private industry infrastructure, both state and local utilities, and the Federal Government, where do you think we are on the conversation level at this point?

Admiral ROGERS. We're having the conversations, clearly. DHS really is in the lead here. We're having the conversation. It's a little uneven, some sectors more than others. But we're all victims of the culture we're from. The culture that I'm from as a uniformed individual is it isn't enough to talk; you must physically get down to execution-level detail about how you are going to make this work, how are we going to coordinate this?

I don't want to get into a crisis and the first time I've dealt with someone is when their network's penetrated. I'm watching data stream out in the gigabit level, and I'm going: so could you tell me about your basic structure? That's not the time to have this dialogue.

Senator LANKFORD. Thank you.

Chairman BURR. Senator Hirono.

Senator HIRONO. Thank you, Mr. Chairman.

Admiral, thank you for your service and for being here today. You and Director Clapper testified before a House committee that

data manipulation and what you refer to as data destruction is probably on the horizon and, while we can't do very much about those kinds of behaviors on the part of non-state actors, isn't it very incumbent on us to engage in discussions and, as some of my colleagues have referred to it, proceeding toward the goal of a cyber arms control agreement with certain state actors who have that capability?

Admiral ROGERS. I don't know if an arms control agreement is the right answer.

Senator HIRONO. Whatever it is, that we come to some kind of understanding so that state actors do not engage in manipulation and destruction of data. I think that would be just totally——

Admiral ROGERS. I would agree. We have been able historically—as a sailor, I can remember at the height of the Cold War we knew exactly how far we could push each other out there. We've got to get to the same level of understanding in this domain, and we are not there right now.

Senator HIRONO. Do you know whether, with the President of China's visit, whether the cyber issues will be discussed by the two leaders?

Admiral ROGERS. I think the National Security Adviser and the President have been very public in saying they will raise the full spectrum of issues, to include cyber, with their Chinese counterparts.

Senator HIRONO. I have a question relating to the OPM breach. Our understanding is that 19 or 20 of 24 major agencies have declared that cyber security is a significant deficiency for their agencies, and you indicated that the NSA doesn't have immediate responsibility to help these other agencies, but that you would respond at the request of DHS. So has DHS made such a request to NSA that you become engaged in helping these other dot-gov agencies to become, well, cyber-safe?

Admiral ROGERS. Not in terms of the day to day per se. There hasn't been a major penetration in the Federal Government in the last 18 months that NSA hasn't been called in to respond. I think the challenge—and I know DHS shares this—is we've got to move beyond the "Cleanup on Aisle 9" scenario, to how to—and it goes to my response to Senator Lankford—how do we get ahead of this problem and start talking to organizations about, what are the steps you need to take now to ensure they can't get in, not, well, they're already in, let me walk you through how to get them out.

Senator HIRONO. Are you engaged in that process now with the 19 agencies?

Admiral ROGERS. Not with every agency in the Federal Government, no.

Senator HIRONO. Why not?

Admiral ROGERS. Again, under the current construct DHS has overall responsibility for the dot-gov domain. For me, I have to be asked.

Senator HIRONO. Well, that was my question.

Admiral ROGERS. Not just unilaterally.

Senator HIRONO. So it's on an agency by agency basis that DHS asks you? And if they were to ask you to deal with all of the dot-gov agencies, would you have the resources to help?

Admiral ROGERS. My first comment would be, we've got to prioritize, because I'm expended to defend all of the dot-mil, and now if there's an expectation that same capacity is also going to work on the dot-gov, my first comment would be we have got to prioritize. What's the most essential things we need to protect?

Senator HIRONO. As I all things, we have to prioritize. But I think that it would behoove DHS—well, it would help if they would make such a request, and then you can engage in prioritizing.

Speaking of resources, I want to thank you for your frank assessment of what would happen if there is a government shutdown. You also indicated in your testimony that recruiting and retaining people is going to be an ongoing challenge for our country to stay ahead in the cyber arena.

I did have the opportunity to visit our very large NSA facility in Hawaii and I thank all the people there for the work that they're doing. But can you talk a little bit about what you're doing, how aggressively you're going after getting the appropriate people to sign on to work for NSA?

Admiral ROGERS. So, knock on wood, both our retention of our STEM, or high technical workforce, continues to be good, as has our ability to recruit. We have more people trying to get in with the right skills than we, quite frankly, have space for right now.

I am always mindful, though, of what are the advance indicators that would suggest that's changing, that we're going to lose more than we can bring in. I would tell you, the workforce at NSA and U.S. Cyber Command still will talk to me about the shutdown in 2013, as an example: hey—I get this every time, literally, when I talk to our workforce around the world: sir, is this going to happen again? Am I going to be told I can't come to work, I may not be paid, or I'm going to be put on furlough again, as we did in 2013? And the situation that we're facing now and what the workforce is reading in the media right now is not helpful.

Senator HIRONO. I agree. Thank you.

Chairman BURR. Senator Cotton.

Senator COTTON. Thank you.

Admiral Rogers, nice to see you in an open setting for once. I've enjoyed our many classified briefings, my visit to your headquarters, and my visits with your many personnel all around the world. On behalf of the three million Arkansans I represent, I want to thank not just you, but more importantly the thousands of men and women you represent. They are patriots, they are professionals, and they're responsible for saving thousands of American lives.

In 2014 North Korea state-sponsored hackers launched a cyber attack against Sony Pictures. Sony responded by quickly calling the FBI and asking for help. My understanding is that Sony chose this course of action largely due to the FBI's expertise in this area, specifically cyber forensic and defense, their belief that a crime had been committed, and because of the strong relationship that they had developed with the FBI. Do you believe Sony did the right thing by calling the FBI?

Admiral ROGERS. I'm not in a position to tell you why they did it. I'm glad they reached out, because then very quickly the FBI reached out to NSA and we ended up partnering. Again, never

thought I would be dealing with a motion picture company about cyber security. But I was grateful for their willingness to be very upfront and very honest: we have received a major penetration with a massive theft of intellectual property and we need help from the government.

Senator COTTON. In the same way that we would encourage a bank that's been held up or a brick and mortar company that's been physically attacked to contact the FBI, you believe that we should encourage these private sector actors to contact the FBI?

Admiral ROGERS. I think the FBI needs to be a part of this. Now, whether it should be DHS, the FBI—part of the things I believe we need to do is we have got to simplify things for the private sector. When I talk to companies around the United States and I'm often approached, hey, can't you do more directly for us, and I'm going, no, I cannot under the current construct, I'm struck by them telling me: you guys have got to make this easier; I can't figure out if I'm supposed to go to the FBI, DHS, do we go to you? Because, for example, I'm in the financial sector, should I go to Treasury?

I think collectively in the government, in the Federal Government, we've got to do a better job of simplifying this so potentially it's one access point and then everything at machine-to-machine speed, to ensure as well accountability and privacy, but the data quickly is disseminated across all of us, because there are so many organizations that to be effective you have to bring to bear in a very orchestrated, very structured way. It can't be like kids with a soccer ball: hey, everybody just runs.

Senator COTTON. The NSA is in charge of information assurance operations for the Federal Government, meaning that the NSA is in charge of assuring our national security systems. Am I correct that NSA from time to time will also help Federal agencies protect their unclassified systems?

Admiral ROGERS. Yes, when they request assistance.

Senator COTTON. I realize this is before your time, but to your knowledge did the State Department ever ask the NSA about the wisdom of setting up a private server so Secretary Clinton could conduct official State Department business?

Admiral ROGERS. I'm not aware of whether they did or they didn't, sir.

Senator COTTON. What would be your response if the current Secretary of State or another Cabinet member came to you and said: Admiral Rogers, I'd like to set up a private, non-governmental server and use that to conduct official business?

Admiral ROGERS. You really want to drag me into this one, sir?

Senator COTTON. I'd simply like your professional opinion.

Admiral ROGERS. My comment would be: you need to ensure you're complying with the applicable regulations and structures for your Department. I'll be the first to admit I'm not smart about what the rules and regulations are for every element across the Federal Government.

Senator COTTON. Are the communications of the seniormost advisers to the President of the United States, even those that may be unclassified, a top priority for foreign intelligence services in your opinion?

Admiral ROGERS. Yes.

Senator COTTON. If an NSA employee came to you and said, hey, boss, we have reason to believe that Russian Foreign Minister Sergei Lavrov or Iranian Foreign Minister Javad Zarif is conducting official business on a private server, how would you respond?

Admiral ROGERS. From a foreign intelligence perspective, that represents opportunity.

Senator COTTON. Are you aware of any NSA officials who emailed Secretary Clinton at her private account?

Admiral ROGERS. No, I have no knowledge. I apologize.

Senator COTTON. Are you aware of any NSA officials who were aware that Secretary Clinton had a private email account and server?

Admiral ROGERS. Now you're talking about something before my time, Senator. I apologize; I just don't know the answer.

Senator COTTON. Could I ask you to check your records and respond back to us in writing, please?

Admiral ROGERS. Yes, sir. I'll take the question for the record.

Senator COTTON. Thank you.

Chairman BURR. Vice Chairman.

Vice Chairman FEINSTEIN. I don't see the relevance of that to this Committee. However, that's just my opinion.

I do have a question. Admiral, you indicated in a private session that you were taking a look at reorganization. I know that isn't completed yet; it's still under way. What can you share with the public about the reasons for it and what you believe it might bring about?

Admiral ROGERS. I've been the Director at NSA now for approximately 18 months and I spent the first portion of those 18 months really focused on the aftermath of media leaks, trying to make sure that we are structured as an organization to deal with that challenge and to make sure that we were in a position to be able to tell our oversight as well as the citizens of the Nation; we are fully compliant with the law and regulation and we're in a place where you should be comfortable that we're able to execute our missions, at the same time ensuring the protection of the data that we access, as well as the broad privacy of U.S. citizens.

I then posed the following question to our workforce: "If we stay exactly the way we are, if we change nothing, in five to ten years are we going to be able to say that we are the world's preeminent SIGINT and information assurance organization?"

I said, "I'm asking you this question because my concern is if we make no changes, I don't think we're going to be able to say that, and I believe that part of my responsibility as a leader is whenever I turn the organizations over I want to be able to tell whoever relieves me: you should feel good that we've structured this so that you're ready to do what you need to do."

As a result of that, I posed a series of questions to the workforce, from how do we build the workforce of the future, to what should our organizational structure look like, to how do we need to optimize ourselves for cyber, because my argument was cyber in the next 15 years will be like counterterrorism has been for the last 15 years; it will be a foundational mission set that drives us as an organization, and it will require us to do things on a scale we've

never done before and to do it more broadly. And to do that, particularly in a declining resource environment, we have got to be more efficient to be effective, guys.

As a result of that, the other point I made to the team was that I don't want this decided by senior leadership at Fort Meade. We're a global enterprise composed of hard-working men and women, and I want them to have a vote, so to speak, an input into what should the organization of the future look like? What do we need to structure ourselves so that in five to ten years, given the changes that we see happening in the world around us, we can say NSA remains the preeminent signals intelligence and information assurance organization in the world?

As a result of that, we spent about six months. The organization, the workforce, has teed up a set of recommendations to me. They probably number in excess of 200. They cover from very minor things to very broad things.

There's three final areas that I said I want you to spend more time on. The first was the military part of the workforce. I tried to remind everybody, as I said in my opening statement to you, we are an enterprise composed of civilian employees, military men and women, active and reserve, officer and enlisted, as well as contractors, and we have to optimize every single part of this enterprise to get where we need to be.

The second issue I said was, I want you to think a little more broadly about cyber, because I don't think we're being far-reaching enough in the recommendations you've given me.

The last one was organizational structure. I said, if you look at—if you were building NSA from the ground up today, is this the structure you would have created? I said, our structure reflects a series of changes and choices that have literally been made over the last 20 years. The last major organizational change at NSA on a wide swath was 1999, 1998, coming up on 20 years ago now, and the world has really changed, and our missions have evolved, and I just want to make sure we're optimized to meet the future.

So I'll receive the final input back on those three by the 1st of October. In fact, I think I'm going to actually review a draft this weekend, to be honest. I'm told they think they have some initial work for me to look at this weekend.

As I had indicated previously, once we sit down and we decide what we think we ought to do, it's my intention to come back to the Committee in its role as oversight to say: this is what's been recommended, this is what I intend to do, here's why I intend to do it, this is what I think it will generate in terms of value.

Vice Chairman FEINSTEIN. Thank you. Thank you. I think NSA is in good hands. Thank you very much.

Chairman BURR. Admiral Rogers, I seldom get the opportunity to highlight North Carolina's high tech successes, especially given the fact that my Vice Chairman represents Silicon Valley. I keep reminding her, I have the Research Triangle Park. But I'd like to note that, while there are 99 days left in the NSA's LTS Net Codebreaker Challenge, that North Carolina State University is currently ranked number one out of 182 entries.

Vice Chairman FEINSTEIN. Is that good?

[Laughter.]

Chairman BURR. It depends on whether the Admiral thinks it's important to please the Chairman.

[Laughter.]

It is good. But I think it highlights again something that Dianne and I both know, that that's the fertile ground that you go to recruit. It's where we develop the next talent that not only works at Research Triangle Park or Silicon Valley, but it works at the NSA, and it really is the backbone of our intelligence organizations.

Admiral, your mission continues to change, in large measure because of the technology explosion. It's an explosion like we've never seen before, really. It'll only speed up; it will not slow down. And your mission will be impacted by that innovation.

I want to say as we conclude, the Committee is here to be a partner. We're anxious to hear your reorganization plans because that reorganization I think gives you the flexibility to move to wherever the challenge forces the NSA to go.

I speak on behalf of the Vice Chairman and myself when I ask you to please go back to the 40,000-plus NSA employees and on behalf of the Committee thank them for the work that they do, work that many times the American people don't understand the value of, but sleep safely at night because of that work.

This hearing is adjourned.

[Whereupon, at 12:24 p.m., the hearing was adjourned.]

○