AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–395

NOMINATION OF LIEUTENANT GENERAL PAUL M. NAKASONE, U.S. ARMY, TO BE DIRECTOR OF THE NATIONAL SECURITY AGENCY AND CHIEF OF THE CENTRAL SECURITY SERVICE

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

THURSDAY, MARCH 15, 2018

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
28–949 PDF WASHINGTON : 2018

SELECT COMMITTEE ON INTELLIGENCE

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

RICHARD BURR, North Carolina, *Chairman*
MARK R. WARNER, Virginia, *Vice Chairman*

JAMES E. RISCH, Idaho
MARCO RUBIO, Florida
SUSAN COLLINS, Maine
ROY BLUNT, Missouri
JAMES LANKFORD, Oklahoma
TOM COTTON, Arkansas
JOHN CORNYN, Texas

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
JOE MANCHIN III, West Virginia
KAMALA HARRIS, California

MITCH MCCONNELL, Kentucky, *Ex Officio*
CHUCK SCHUMER, New York, *Ex Officio*
JOHN MCCAIN, Arizona, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*

CHRIS JOYNER, *Staff Director*
MICHAEL CASEY, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

MARCH 15, 2018

OPENING STATEMENTS

Burr, Hon. Richard, Chairman, a U.S. Senator from North Carolina 1
Warner, Mark R., Vice Chairman, a U.S. Senator from Virginia 2

WITNESS

Nakasone, Lieutenant General Paul M., U.S. Army, Nominated to be Director of the National Security Agency and Chief of the Central Security Service ... 4
Prepared statement 7

SUPPLEMENTAL MATERIAL

Questionnaire for Completion by Presidential Nominees 26
Additional Prehearing Questions 42
Questions for the Record 59
Statement from the Electronic Privacy Information Center 71

NOMINATION OF LIEUTENANT GENERAL PAUL M. NAKASONE, U.S. ARMY, TO BE DIRECTOR OF THE NATIONAL SECURITY AGENCY AND CHIEF OF THE CENTRAL SECURITY SERVICE

THURSDAY, MARCH 15, 2018

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

The Committee met, pursuant to notice, at 10:03 a.m. in Room SH–216, Hart Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Present: Senators Burr, Warner, Risch, Blunt, Lankford, Cotton, Wyden, King, and Harris.

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. Lieutenant General Paul M. Nakasone, President Trump's nominee to be the next Director of the National Security Agency, General Nakasone, congratulations on your nomination.

I'd like to start by recognizing your wife Susan. She's here with us today and your four children: David and Joseph, who are both high school juniors; Sarah, who's studying at the University of Chicago; and Daniel who is at the University of Virginia. You've got them geographically spread around. I know from personal experience just how important a supportive family is. And to each of you—and, Susan, I hope you pass it on to the kids—thank you.

Our goal in conducting this hearing is to enable the committee to consider the nominee's qualifications and to allow for thoughtful deliberation by our members. Lieutenant General Nakasone has provided substantive written responses to over 45 questions presented by the committee. And today, of course, committee members will be able to ask additional questions and hear from him in open session.

General Nakasone graduated from Saint John's University and earned a master's degree from the University of Southern California, the National Defense Intelligence College, and the United States Army War College. He served honorably in the United States Army for over 30 years, including deployments to Afghanistan, Iraq, and the Republic of Korea. Prior to leading the United States Army Cyber Command, General Nakasone commanded the

Cyber National Mission Force at the United States Cyber Command.

General Nakasone, you are being asked to lead the National Security Agency during a period of significant debate about what authorities and tools are lawful and appropriate. I'm hopeful that, moving forward, you will be an influence and an influential and forceful advocate for those foreign intelligence tools you believe are necessary to keep the citizens of this country safe while protecting Americans' privacy.

As I have mentioned to others during their nomination hearing, I can assure you that this committee will faithfully follow its charter and conduct a vigorous and real-time oversight of the intelligence community, its operations and its activities. We'll ask difficult and probing questions of you and your staff and we will expect honest, complete and timely responses.

You've already been reported favorably out of the Senate Armed Services Committee on 6 March of this year, and I look forward to supporting your nomination and ensuring its consideration without delay.

I want to thank you again for being here. I look forward to your testimony.

Finally, yesterday the committee received a statement from the Electronic Privacy Information Center and asked that it be entered into the hearing record. I would ask members for unanimous consent that that statement be entered into today's open record. Hearing no objection, so ordered.

I now recognize the Vice Chairman for his lengthy comments.

[Laughter.]

OPENING STATEMENT OF HON. MARK R. WARNER, VICE CHAIRMAN, A U.S. SENATOR FROM VIRGINIA

Vice Chairman WARNER. Thank you, Mr. Chairman. Since no one is here, I'm sure people are going to be hanging on my every word.

General Nakasone, it's great to see you again and welcome. I believe actually, since you're the first director as—as Director of NSA and CYBERCOM, this is the first time, though, as NSA Director that you've appeared before the committee. So a bit of a historic hearing; and, consequently, slightly extended remarks of mine.

Obviously, General, if you are confirmed you will take charge of one of the most important assignments in our government and in the intelligence community. You will be entrusted to lead thousands of dedicated men and women of the NSA. It will be your job to ensure accurate and timely signals intelligence is provided to our Nation's leaders and warfighters.

You'll be responsible for protecting our military networks, safeguarding the unique capabilities and assets of the United States, and outsmarting our adversaries. And, as Commander of U.S. CYBERCOM, you will also be responsible to—for responding to threats and conduct operations when ordered to do so.

At the same time, as we've discussed again, you must ensure that the NSA operate within the law and that it continues to protect the privacy and civil liberties of Americans. The NSA's activities must continue to operate within the parameters of that law, particularly the FISA law, with foolproof mechanisms for ensuring

that no Americans are targeted without warrant, and will continue to be subject to robust oversight by this committee.

Your nomination I believe comes at a critical time. As I look around the world, I see threats and challenges to our country, to our systems of international institutions and alliances, that frankly have maintained peace and prosperity since World War II. We've also seen domestic threats to the NSA's ability to execute on its mission, with a series of leaks that have challenged the agency and at times undermined the morale of your workforce.

The NSA must provide the best intelligence on terrorists and extremist groups, rogue regimes, nuclear proliferation, and regional instability. I'm concerned about the rise of potential nation-state adversaries and their policies which aim to disrupt the international order.

In particular, we should all be alarmed by the destabilizing role played by Vladimir Putin's Russia, which threatens both the United States and our allies and, as we've seen by their recent activities in the U.K., there are very few restrictions that Mr. Putin has put on his agent's actions. Matter of fact, the heads of our intelligence agencies were here a month ago and all indicated that Russia will continue to try to interfere in our elections, activities that demand a strong United States response.

Our country I believe must develop a whole-of-government response to strengthen our defenses. I believe—and we've again discussed this, we'd like to hear more about this today—that we need a clearly articulated cyber doctrine that will deter nations like Russia from going after our crucial institutions, whether they be civilian, military, or in the private sector. We've got to make sure they know, whether it's Russia or other near-peer adversaries, that there will be consequences to their actions.

I believe that our lack of action to date has, frankly, encouraged nations not only like Russia, but China and others, frankly to act with impunity. I also worry that we're on the cusp of what I would call a paradigm shift in the technological development, and not one which we're well-poised to prevail against well-resourced competitors, who are willing to engage not only in a whole-of-government, but particularly a whole-of-society effort, to obtain economic advantages and access to our most sensitive technologies.

The top dozen Chinese technology firms that have already entered or are poised to enter the United States and Western markets, in stark contrast to our country, these firms maintain relationships with and provide access to the Chinese government that is unlike anything we've seen with other developed nations. While we want to encourage an open economy, what are the potential risks to our society from these developments?

Now, China is still behind the United States in R&D expenditures, but, with the current spend lines, not for long. China's R&D spending is increasing by about 20 percent a year. By comparison, our R&D expenditures are increasing about 4 percent a year.

Frankly, the lines will shortly cross; and China is positioning itself to be a global leader in artificial intelligence, quantum computing, and bioengineering, and that brings serious implications for our privacy, economic and national security. I believe the NSA will

continue to play a critical role in keeping our country ahead in this ever-changing world of emerging technologies.

Finally, I'd like to hear your thoughts about the dedicated men and women of the NSA, your workforce of dedicated intelligence professionals. These are men and women who work in silence to keep America safe. Now, they've taken a beating sometimes recently from those who falsely call into question their motivations, their dedication and their honesty. I know that these attacks obscure the truth.

My colleagues on this committee and I know that at the NSA headquarters the Memorial Wall lists the names of 176 NSA cryptologists, military and civilian, who made the ultimate sacrifice for their country while serving in silence. I'd like to hear your plans on how we maintain that world-class workforce going forward.

Again, thank you, Mr. Chairman, for holding this hearing and I look forward to the General's comments.

Chairman BURR. I thank the Vice Chairman.

General, if you would stand and raise your right hand. Do you solemnly swear to tell—to give this committee the truth, the full truth and nothing but the truth, so help you God?

General NAKASONE. I do.

STATEMENT OF LIEUTENANT GENERAL PAUL M. NAKASONE, U.S. ARMY, NOMINATED TO BE DIRECTOR OF THE NATIONAL SECURITY AGENCY AND CHIEF OF THE CENTRAL SECURITY SERVICE

Chairman BURR. Please be seated.

General, before we move to your statement, I'll ask you to answer five standard questions the committee poses to each nominee who appears before us. They require a simple yes or no response for the record.

Do you agree to appear before the committee here or in any other venue when invited?

General NAKASONE. Yes.

Chairman BURR. If confirmed, do you agree to send officials from your office to appear before the committee and designated staff when invited?

General NAKASONE. Yes, Mr. Chairman.

Chairman BURR. Do you agree to provide documents or any other materials requested by the committee in order for it to carry out its oversight and legislative responsibilities?

General NAKASONE. Yes, Mr. Chairman.

Chairman BURR. Will you ensure that your office and your staff provide such materials to the committee when requested?

General NAKASONE. Yes, Mr. Chairman.

Chairman BURR. Do you agree to inform and fully brief, to the fullest extent possible, all members of this committee on all intelligence activities, rather than only the Chair and the Vice Chair?

General NAKASONE. Yes, Mr. Chairman.

Chairman BURR. Thank you very much for your answers. We'll now proceed to your opening statement, after which I'll recognize members by seniority for up to five minutes. General, the floor is yours.

General NAKASONE. Chairman Burr, Vice Chairman Warner, and distinguished members of the committee: I am honored to testify here today for my nomination as Director of the National Security Agency and Chief, Central Security Service. I want to thank President Trump, Secretary Mattis, Director Coats, and General Dunford for their confidence in nominating me for these important positions.

I'd also like to thank my wife Susan for being here. I owe much of my success to her love and support throughout nearly 25 years of marriage. Today, our children, Sarah, Daniel, David and Joseph, are all in school and will be unable to be with us. We're tremendously proud of them and thankful for their selflessness and support.

I'd also like to thank Admiral Mike Rogers for his 36 years of commissioned service for the Nation, and for leading NSA during a time of incredible transformation and tremendous growth. I thank him and his wife Dana for all they have done in service to our Nation.

I commissioned in the Army over 31 years ago as an intelligence officer and for the past three decades, have served in intelligence and in leadership positions both at home and abroad, in peace and in war.

If confirmed for this position, this will be my fourth assignment to NSA. In my previous assignments to the agency, I've always been impressed by the phrases that greet everyone who enters that building: "Defend the Nation, secure the future." These simple directives captured the critical role the NSA plays in supporting our military and senior policymakers while safeguarding our freedoms.

I know that the National Security Agency is a special member of our intelligence community and of unique importance in the defense of our Nation. Throughout the agency's 65 years of service, one constant has remained—the quality of the people. These men and women are national treasures and they're engaged in missions that can only be called one of a kind. If confirmed, I know this workforce will be the foundation of NSA's future and continued success. My focus will begin and end with them.

Throughout my career, I've been both a generator and consumer of NSA intelligence products and know first-hand the critical role the agency plays, both as a combat support and signals intelligence agency. The importance of delivering accurate, reliable and timely intelligence products cannot be overstated. And, if confirmed, I commit to upholding the high reputation of the agency as a provider of objective, mission-critical signals intelligence in support of our military and our government.

I recognize that our Nation's adversaries continue to pose threats and posture themselves to reduce our global advantage. In light of this, the importance of an effective National Security Agency continues to be paramount to our national defense.

I also recognize that we are at the edge of the technological frontier for our Nation. The future that the next director will face presents challenges and opportunities from rapid technological evolution, including machine learning, artificial intelligence and quantum computing, as well as the growing capabilities of the technological industry. If confirmed, I know that a strong public-private

partnership will be needed to ensure this country benefits from the leading-edge technology being developed and implemented today and into the future.

Finally, I recognize that this nomination is to lead both U.S. Cyber Command and the NSA. Although the co-location and cooperation of the two powerful organizations has been critical to their growth, I also see them as two unique entities with their own identities, authorities, and oversight mechanisms. I am committed to assessing the needs of both to optimize their individual success in the best defense of our Nation.

If confirmed, I will ensure that the agency's intelligence customers can continue to rely upon timely and accurate products, delivered with integrity, to ensure we maintain an advantage over increasingly adaptive adversaries. Equally, I will always ensure the National Security Agency upholds full compliance with our laws and the protection of our constitutional rights.

I am deeply honored to be considered for these leadership positions. If confirmed, I look forward to working closely with the committee and the entire Congress to ensure we leverage our opportunities and also address our challenges. Chairman Burr, thank you for this opportunity to be here this morning. I look forward to answering your questions.

[The prepared statement of General Nakasone follows:]

15 MARCH 2018

LTG PAUL M. NAKASONE

SSCI NOMINATION HEARING – OPENING REMARKS

Chairman Burr, Vice-Chairman Warner, and distinguished members of the Committee, I am honored to testify here today for my nomination as Director of the National Security Agency, and Chief, Central Security Service.

I want to thank President Trump, Secretary Mattis, Director Coats, and General Dunford for their confidence in nominating me for these important positions.

I'd like to also thank my wife Susan for being here. I owe much of my success to her love and support throughout nearly 25 years of marriage. Susan and I are joined today by our children David and Joseph. We're tremendously proud of them, as well as our children Sarah and Daniel, who are away at college and couldn't make it here today.

I want to thank Admiral Michael Rogers for his 36 years of commissioned service to our Nation, and for leading NSA during a time of incredible transformation and rapid growth. I thank him and his wife Dana for all they have done in service to our Nation.

I commissioned in the Army over 31 years ago as an intelligence officer, and for the past three decades have served in intelligence and leadership positions both at home and abroad, in peace and in war.

If confirmed for this position, this will be my fourth assignment to NSA. In my previous assignments at the Agency, I have always been impressed by the phrases that greet everyone who enters the building: "Defend the Nation; Secure the Future." These simple directives capture the absolutely critical role the National Security Agency serves to support our military and senior policy makers while safeguarding our freedoms.

I know that the National Security Agency is a special member of our Intelligence Community and of unique importance in the defense of our Nation. Throughout the Agency's 65 years of service, one constant has remained—the quality of the people who work there. These men and women are national treasures and they are engaged in missions that can only be called, one-of-a-kind. If confirmed, I know this workforce will be the foundation of the NSA's future and continued success. My focus will begin and end with them.

Throughout my career, I have been both a generator and consumer of NSA intelligence products, and know first-hand the critical role the Agency plays as both a combat support and signals intelligence agency. The importance of delivering accurate, reliable, and timely intelligence products cannot be overstated, and if confirmed I commit to

upholding the high reputation of the Agency as a provider of objective, mission-critical signals intelligence in support of our military and our government.

I recognize that our Nation's adversaries continue to pose threats and posture themselves to reduce our global advantage. In light of this, the importance of an effective National Security Agency continues to be paramount to our national defense.

I also recognize that we are at the edge of the technology frontier for our Nation. The future that the next Director will face presents challenges and opportunities from rapid technological evolution including machine learning, artificial intelligence, and quantum computing, as well as the growing capabilities of the technology industry. If confirmed, I know that a strong public-private partnership with our Nation's private sector will be needed to ensure this country benefits from the leading-edge technology being developed and implemented today and into the future.

Finally, I recognize that this nomination is to lead both U.S. Cyber Command and the NSA. Although the co-location and cooperation of the two powerful organizations has been critical to their growth, I also see them as two unique entities, with their own identities, authorities, and oversight mechanisms. I am committed to assessing the needs of both to optimize their individual success in the best defense of our Nation.

If confirmed, I will ensure that the Agency's intelligence customers can continue to rely upon timely and accurate products, delivered with integrity, to ensure we maintain an advantage over increasingly adaptive adversaries. Equally, I will always ensure the National Security Agency upholds full compliance with our laws and the protection of our Constitutional rights.

In closing, I am deeply honored to be considered for these leadership positions. If confirmed, I look forward to working closely with this committee and the entire Congress to ensure we leverage our opportunities and also address our challenges. Chairman Burr, thank you for the opportunity to be here this morning. I look forward to answering your questions.

Chairman BURR. General, thank you for that statement. Thank you for your service to the country. One could leave with what you have accomplished, with a great career; but I think greater things are ahead of us for you and for this country. And we're grateful for your willingness and your family's willingness to take this next chapter.

Before we begin, I'd like to advise members that, pursuant to Senate Resolution 400, the committee received this nomination on referral from the Senate Armed Services Committee on 6 March 2018 and we have 30 calendar days within which to report this nomination to the full Senate. It is my intention to move to a committee vote on this nomination as soon as we possibly can. Therefore, for planning purposes, if any members wish to submit questions for the record after today's hearing, please do so by close of business today.

With that, we will go into the five-minute round by seniority, and I'll recognize myself first.

General, leaks of classified information this committee takes very seriously; and we believe it puts sensitive sources and methods at risk and can in many cases cause irreparable damage to our national security. Our committee has already taken action in the Intelligence Authorization Act for fiscal year 2018 by imposing enhanced penalties on those convicted of unauthorized disclosures. If confirmed, how do you plan to address the security of sensitive and classified information at the agency?

General NAKASONE. Mr. Chairman, the safeguard of our national secrets, the safeguard of our capabilities, is one of the most important things the next director will continue to address. If confirmed, my intent is to look to make sure that the "Secure the Enterprise" and the "Secure the Network" initiatives that NSA has undertaken to date are timely, are accurate, are on target, to ensure that we continue to have the safeguard and security of our national treasures.

With that being said, I would also add, Mr. Chairman, that there are two elements that I see as we look long-term to this issue. First of all is continuing to hire great people that work at the NSA, not only hiring them but also training them, developing them, and ensuring that their long-term careers with the NSA are well tended to.

The second thing, though, is we need to also understand that there are control mechanisms that we as an agency need to continue to look at to ensure that we have the ability to not only safeguard our network, but also secure our environment.

Chairman BURR. General, do I have your commitment that, if such a leak happens, that you will, as timely as you can, notify the committee? And will you continually notify the committee on progress that NSA makes towards preventing and deterring unauthorized leaks?

General NAKASONE. Certainly, Mr. Chairman.

Chairman BURR. Thank you.

General, the committee Intel Authorization Act of 2018 and fiscal year 2017 included provisions to enhance NSA's ability to recruit and retain science, technology, engineering, and mathematics—STEM—employees. Nevertheless, NSA employees still will be com-

pensated less than their private sector counterparts. How do you plan to recruit and retain those top STEM candidates, especially given that there is that compensation gap between government and the private sector?

General NAKASONE. Mr. Chairman, first of all thank you to the committee for the Intelligence Authorization Act. I think that is a very, very important element, important ability for the next director to be able to leverage in the future.

As I take a look at NSA's workforce and my previous experience, the one thing that sets NSA apart is their mission. I believe the most critical thing that we have to continue to do at the National Security Agency is to ensure our people understand and are able to work this very important mission: Defend the Nation, secure the future. This is what I think is essential for us and is our advantage as we look to the future.

Mr. Chairman, I would also say as we look to the future we have to continue broad abilities to recruit from a very, very diverse population, academia, industry, inside our government. I think this is critical that we can continue to attract our best and brightest people.

Chairman BURR. General, are you familiar with NSA21?

General NAKASONE. Yes, Mr. Chairman, I am.

Chairman BURR. Would you just briefly comment on your views on that initiative, which is to prepare for the 21st century a more efficient, effective NSA?

General NAKASONE. Mr. Chairman, NSA21, as I understand it, the largest reorganization of the agency since 2000. And that's significant if you consider the fact that 70 percent of the agency has been hired since 9/11. It was designed to improve, obviously, and focus on people, integration, and innovation. It was designed to address a number of changes in our environment, changes to our networks, changes to competition for our workforce, changes to our budget.

I would say to date, it has just been instantiated at the end of 2017. And so, if confirmed, I would ask if I could have a bit of time to take a look, evaluate what has been done, look at what has been successful and what may need assessment and continue that dialogue with the committee.

Chairman BURR. You've got a commitment to do that.

With that, my time's expired. The Vice Chairman.

Vice Chairman WARNER. Thank you, Mr. Chairman.

And again, General, congratulations on your nomination and thank you for your service. One of the things I think this committee prides itself on is our strong working relationship with all components of the intelligence community. And as you're aware, we have had an ongoing investigation into Russian activities stemming from the 2016 election. For the record, will you commit to ensuring that this committee will be provided with all the information requested pursuant to our ongoing Russia investigations?

General NAKASONE. I will, Mr. Vice Chairman.

Vice Chairman WARNER. Thank you.

At our last open hearing, we had all of the heads of all the principal intelligence community agencies. Every one of them, including your predecessor Admiral Rogers, reconfirmed their support for the

January 2017 assessment that Russia interfered in our last elections.

I want to get in, for the record: Do you agree with that January 2017 IC assessment, that Russia interfered in our 2016 elections? And the second part, editorial comment here: In light of their success in those efforts, do you expect further interference by Russia in our elections and, for that matter, the elections of our allies?

General NAKASONE. Mr. Vice Chairman, I agree with the 2017 assessment. I think the Director of National Intelligence has said it best with regards to future actions of the Russians. And that is, "Unless the calculus changes, that we should expect continued issues."

Vice Chairman WARNER. Well, we would look forward to working with you on making sure—this committee is going to have a public hearing next week on this issue of election security, and I'm very proud of members of both sides of the aisle and how hard they've worked on that. And we, if confirmed, would look forward to working with you on this issue of election security.

One of the things that I've found and believe is that we don't have, I think, a clearly articulated cyber doctrine at this point that not only defends our government, but also deters particularly near-peer adversaries. I think I could better articulate our strategy vis-à-vis second-level states like North Korea, Iran, and terrorist threats like ISIS. But I am concerned with near-peer adversaries we don't have that clear cyber doctrine.

And I know you're just coming into this position, but who do you think in the Administration is in charge of developing a cyber doctrine policy that would deter, whether it's Chinese theft of our intellectual property or Russia misinformation and disinformation campaigns. Who's going to be in charge of developing that doctrine and where do you think it stands at this point?

General NAKASONE. Senator, ultimately I would anticipate that strategies such as this would come from the Executive Branch, perhaps the National Security Council. However, I would anticipate that all elements of the government would contribute to the strategy.

In terms of, if confirmed, my role, I would anticipate that I would provide my insights to both the Joint Staff and the Department of Defense as this strategy is developed.

Vice Chairman WARNER. Well, with your strong intelligence background, I hope we can count on you to be part of that. I think it is time that we have that clearly articulated doctrine. And again, this is not a criticism in this case of the current Administration. This has been a problem, I think, that has plagued our Nation for more than a decade.

One of the areas that I constantly come back to and I think is an example of where we need a doctrine is with how we deal with the dramatic increases of devices that are connected to the internet, the so-called Internet of Things. We're roughly at about 10 billion devices connected now. That number is estimated to go to 20 to 25 billion within the next five or six years. Matter of fact, the Director of the DIA, General Ashley, emphasized that our weakest technology components, mobile devices and the Internet of Things, was an area of exploitation for potential adversaries.

How do you think we would go about securing devices connected to the internet? And do you think that there ought to be at least a basic policy put in place that would say that the Federal Government's purchasing power ought to be used with some determination that we only would buy devices that, for example, are patchable or don't have embedded pass codes so that we don't, frankly, embed within our Federal Government enormous new vulnerabilities?

General NAKASONE. So, Senator, certainly awareness, as you talk about, the Internet of Things is very important for all of us to understand both the opportunities and certainly the challenges here. I think there will likely be, obviously, movement that will have to come from the private sector on this.

In terms of policy decisions, I would defer that to the Department of Defense as they weigh in to this. But my sense is that we have to have a very candid discussion about the growth, the explosion of the Internet of Things, and most importantly the impact that it could have on our economy and certainly our national security.

Vice Chairman WARNER. Well, again, I think you can play a critically important role here. I just would hate for us five years from now to realize we've bought literally billions of devices, just within the Federal Government, and they have actually increased our vulnerability. Thank you for your responses.

Thank you, Mr. Chairman.

Chairman BURR. Thank you, Vice Chairman.

Senator Blunt.

Senator BLUNT. General, let's just start where Senator Warner did. You know, Admiral Rogers, who we all have great respect for, got a lot of attention recently, I believe on the House side, saying he'd been given no new directions as to how to deal with things like Russian interference in the elections. So let's—let's take that in two directions.

One is, do you need any new direction, in your view, to deal with defending against those kinds of attacks? Do you have all the defensive authorization you need? Not whether you have all the equipment and staff you need, but do you—do you have all the authorization you need to defend our institutions against outside aggression?

General NAKASONE. So, Senator, certainly in terms of defending the Department of Defense networks, I think that there are all the authorizations and policies and authorities that are necessary.

Senator BLUNT. What do you need about the non-department? NSA, what if somebody's attacking the—the State Department or some other?

General NAKASONE. So certainly, if confirmed as the Director of the National Security Agency, the authorities for the national security systems falls within the purview of the Director of NSA and I believe has the authorities on which he would be able to execute that defense.

Senator BLUNT. Do you need more authorities to work with State and local election officials?

General NAKASONE. So certainly, there would need to be a policy decision, Senator, that would indicate that that there would be, you

know, more authorities for—for Cyber Command or NSA to be able to do something like that.

Senator BLUNT. But for the Federal Government and for the military, your defensive role is clearly understood?

General NAKASONE. So certainly for—on the NSA side for the national security systems, it is understood; and on the CYBERCOM side for the defense of DOD networks, certainly understood.

Senator BLUNT. And I think we all, and I believe this was Senator Warner's question, well, worded maybe a little bit differently: How do we develop a more well-understood response, an offensive guideline, if you would? How do we—what do we need to do to be sure that our adversaries know that there's a price to be paid, beyond just us trying to subvert their efforts to get into our networks? Do we have an offensive strategy and do we need one?

General NAKASONE. So, Senator, I think both Vice Chairman Warner and yourself speak to this idea of a strategy: What is the strategy for the Nation in terms of cyberspace? I think that strategy being developed in terms of how we defend ourselves, certainly, is important, and it would lay out roles, responsibilities, functions of the major elements of our government.

And I think that that is obviously one of the things that would help both internally for the elements of our government, but also externally, as you say, to provide a set of left and right boundaries perhaps for our adversaries to understand.

Senator BLUNT. Well, I think a determination to create where those boundaries are and what we might do may need to be made outside of your agency. But inside your agency, I can't imagine a more important person to be at the table when we try to determine what—how that—how that determination could actually be implemented. I think there's a strong sense that there's too much of no price to be paid at this point by people who try to either steal our intellectual property, or interfere with elections, or whatever else they might try to do.

The other area where I think you may have to look for an even more expansive role is the acquisition of equipment, signal intelligence equipment, by other agencies. I think you have a role to play there in one of the many hats you'll be wearing in this job. Do you have concerns that other Federal agencies may be buying equipment that could in the future be troublesome for us?

General NAKASONE. Senator, I certainly have concerns. I think the recent statements by the Department of Homeland Security and their directives with regards to select antivirus companies throughout the world and the ensuing National Defense Authorization Act that prohibited the use of select antivirus products within our government is very, very important for the future.

Senator BLUNT. Well, again, I think you bring the information to the table on that.

And my last question would be something we've talked about before. Particularly at the Cyber Command level, what's the value of the Reserve force or the National Guard? I know Missouri has a really good cyber unit. I think cyber units in the Reserves, back to maybe the Chairman's question about how we have the talent we need: How do we bring that part-time talent to use to our benefit, if that's a good idea in your opinion?

General NAKASONE. Senator, I think it's a tremendous idea. In my current role as the Commander of Army Cyber, our Army is building 21 cyber protection teams, 10 in the U.S. Army Reserve and 11 in the National Guard. What you indicate is critical for us as we look to increase the best and brightest of our Nation being able to commit to the defense of our Nation in cyberspace. The Guard, the Reserve, have tremendous talent that we look to in the future to provide us what we often term the strategic depth for our Nation. And so very, very pleased to serve with those fine Americans and hopefully in the future continue to be able to incorporate and to promote their service for our Nation.

Senator BLUNT. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Thank you.

Senator Wyden.

Senator WYDEN. Thank you very much, Mr. Chairman. Mr. Chairman and colleagues, just a quick comment before we go to our nominee. The nomination of Gina Haspel to head the CIA comes at an especially momentous time. Senator Heinrich and I have asked that certain aspects of her background be declassified so that the American people can see what sort of person might head the agency at a particularly important time. I'll just wrap up this point by saying I hope members will support what Senator Heinrich and I are calling for with respect to declassification.

Mr. Nakasone, a historic day because, as I understand it, you are the first nominee from the NSA to be considered at this committee; and we welcome you; and let me begin with some questions.

In 2001, then-President Bush directed the NSA to conduct an illegal, warrantless wiretapping program. Neither the public nor the full Intelligence Committee learned about this program until it was revealed in the press. Speaking personally, I learned about it from the newspapers.

So there is a lot riding on how you might address a similar situation, and we've already noted the history of your being here. If there was a form of surveillance that currently requires approval by the FISA Court and you were asked to avoid the court based on some kind of secret legal analysis, what would you do?

General NAKASONE. Senator, thank you for that question. First, I would offer, with regards to the situation that you describe, I would obviously have a tremendous amount of legal advice that would be provided to me, if confirmed, by those in the agency, by those in the department, by those obviously that are in the Director of National Intelligence.

At the end of the day, I think that one of the most important things is that we have the conversation between the National Security Agency and this oversight committee to understand——

Senator WYDEN. Let me just stop it right there, so I can learn something that didn't take place before. You would, if asked, tell the entire committee that you had been asked to do that?

General NAKASONE. So, Senator, I would say that I would consult with the committee. I would obviously ensure——

Senator WYDEN. Would you inform—when you say "consult," you would inform us that you had been asked to do this?

General NAKASONE. So, again, Senator, I would consult with the committee and have that discussion. I think that one of the important things that I have seen is the relationship between the National Security Agency and this committee. My intent would continue that, that discussion.

But at the end of the day, Senator, I would say that there are two things that I would do: I would follow the law; and I would ensure, if confirmed, that the agency follows the law.

Senator WYDEN. First of all, that's encouraging, because that was not the case back in 2001. In 2001, the President said: We're going to operate a program that clearly was illegal, illegal. You've told us now you're not going to do anything illegal. That's a plus. And you've told us that you would consult with us if you were ever asked to do something like that. So I appreciate your answer.

Now let me move next to encryption. The widespread consensus from encryption experts is that tech companies can't modify their encryption to permit law enforcement access to Americans' private communications and data without also helping sophisticated foreign government hackers get in. You are as familiar with the capabilities of our adversaries as anybody. Do you agree or disagree with those experts?

General NAKASONE. So, Senator, in terms of encryption I would begin with saying this is something that for 65 years NSA has been at the forefront of doing, encrypting our national security systems, our data, our information, our networks. What has changed these days is the fact that the power of encryption, particularly in the private sector, has put law enforcement at times, even with a court order, at risk of being able to—be able to investigate or perhaps even prosecute a crime.

I would offer that for the future this is one of those areas that, if confirmed, I have much to learn and——

Senator WYDEN. My time—my time is up, General. Just a yes or no answer to the question with respect to what experts are saying. Experts are saying that the tech companies can't modify their encryption to permit law enforcement access to America's private communications without the bad guys getting in, too. Do you disagree with the experts? That's just a yes or no.

General NAKASONE. So I would offer, Senator, that it's a conditional yes; that there are times when——

Senator WYDEN. Right. That is—that's encouraging as well. I look forward to working with you in the days ahead.

Thank you, Mr. Chairman.

Chairman BURR. Senator Lankford.

Senator LANKFORD. General, thank you. Thanks for your service in the past and I appreciate you stepping up into this role. The nomination process is not a fun process. It's not someone, anyone, wakes up and says: Gosh, I'd like to go through Senate confirmation, because of the length of the investigation, the information you've already put out, and the questioning time. So I just want to tell you, I appreciate you doing it and stepping up to work through the long, difficult process.

Help me understand the role of collaboration between the NSA and commercial entities and their networks, critical infrastructure and their networks, just the communication in trying to be able to

determine real threats that are there that we may face domestically or internationally?

General NAKASONE. Senator, in terms of collaboration, so NSA for many, many years has been at the forefront obviously of understanding advances of our—of our adversaries. That reporting, that communication with other elements of our government, whether or not it's the Federal Bureau of Investigation or it's the Department of Homeland Security, has been critical to inform other members of our critical infrastructure and key resources.

I see this as an element that must continue into the future and a sharing and integration that's important for the overall defense of our Nation.

Senator LANKFORD. How do we get that faster? What does it take to have faster collaboration?

General NAKASONE. So I think faster collaboration is driven by, you know, several things. One is a demand signal, a demand signal that's coming from not only other elements of our government, private sector. I would also say that it's—it's also part of supply, being able to grow a number of analysts and an ability to continue to report. I think those are two of the key elements, Senator.

Senator LANKFORD. So let's talk about this wonderful term that's thrown around NSA all the time, the "dual hat," working with U.S. Cyber Command and then also directing the NSA. You made a comment in your opening statement about that, that that has been and will continue. But you also made a comment that you see those as unique entities.

Help me understand a little bit. Are there walls between those two entities, or are they just distinct roles, or how do you see them as unique entities?

General NAKASONE. Senator, if I might begin with the dual hat discussion. In terms of the dual hat arrangement, I'm not predisposed in terms of whether that arrangement stays or ends.

Senator LANKFORD. Right.

General NAKASONE. I know that the President and Congress both have spoken on it, the President in August of 2017 and then Congress in the NDAA that listed a series of six conditions that both the Secretary and the Chairman must attest to before the dual hat is terminated.

It's my assessment that what we should do at the end of the day is make a determination that is in the best interest of the Nation. That's the key, critical piece of it. If confirmed, my intent would be to spend the first 90 days looking at that, providing an assessment to both the Secretary and the Chairman, and then moving forward from there.

Senator LANKFORD. Okay. Would you allow us to be in that conversation as well, as far as your assessment?

General NAKASONE. Certainly, after talking with the secretary and the Chairman, yes, Senator.

Senator LANKFORD. That's fine. That'd be just fine.

So talk to me a little bit about this issue about cyber doctrine. That is something this committee has talked about often. It has been something that has been a frustration. I'm just trying to see who is giving recommendations to the President on how we respond, the speed of our response. Attribution for where attacks

came from are difficult to do, as you know extremely well. But, if we don't get a quick response to that and individuals aren't able to make decisions with accurate, timely information, it makes it much tougher.

So the question that we always have is who makes the call? Who is it that presents the set of ideas to the President to say, here are the options that you have? Where does—where do you expect that comes from?

General NAKASONE. Senator, if I might begin with the strategy or the doctrine piece and then, with regard to the options, address that as well. I do believe that an overall strategy for how the Nation is going to defend itself in cyberspace is very important. What are the roles of the Department of Defense, the Department of Justice, and Federal Bureau of Investigation and, of course, the Department of Homeland Security? How do we ensure that there's cross talk, that there's obviously roles and responsibilities that are—that are fully delineated? I think that's an important piece.

With regards to options in the future, if confirmed I would see that as my role as Commander of U.S. Cyber Command to prove a series of options within cyberspace that the Secretary of Defense and the President can consider. I would offer, however, that—that that may not be the only set of options that are necessary. When we look at the strength of this Nation, the Nation has tremendous strengths diplomatically, informationally, economically, and those might also be options presented.

Senator LANKFORD. But who's the clearinghouse to be able to gather those and be the final presentation to the President?

General NAKASONE. So, in terms of military options, Senator, I think that would be myself to the Secretary of Defense and then the President.

Senator LANKFORD. Okay. That's what we need to hear. Thank you very much.

Chairman BURR. Senator King.

Senator KING. Thank you, Mr. Chairman.

Following-up on that question, I think this is one of the most important areas of policy. Just moments ago, we received information that the United States Government has imposed additional sanctions on Russia in response to the activities in 2016. The question is, are sanctions enough? Sanctions are important, but the question is sanctions always, by definition, occur after the attack. The best attack is the one that doesn't occur.

That gets to the question of deterrence. And I hope, as we discussed in the Armed Services Committee, one of the tasks you will take on is doing just what you said, of developing options that would be available to us, that we could talk about as deterrence. Your thoughts on the importance of having some deterrent capability, as well as after-the-fact punishment capability?

General NAKASONE. Senator, I agree in terms of having a range of options, and I would certainly see, if confirmed, my role to provide a series of cyber options that might be used in a deterrent role.

But I think it's important to state that it's not only cyber or military options that may be the most effective. And, in fact it may be less effective than other options that might be considered. And so

I think that that's an important piece that, you know, as we consider the future, what are the range of options that might include the entire government is critical for us.

Senator KING. And I agree. I'm not—I'm not suggesting that it has to be cyber for cyber or military for military. But the point is, adversaries have to know they will pay a price for attacking us, whether it's cyber or kinetic.

General NAKASONE. I agree, Senator.

Senator KING. And also, it was mentioned in this morning's press conference apparently, and I just have one sentence on this, the Administration has warned the country about potential attacks on critical infrastructure, particularly the electric grid. My concern is that the electric grid is not only vulnerable; but, from public reports, that there are already efforts to plant malware or to seed malware in SCATA systems, et cetera. Is this something that you're familiar with and are concerned about?

General NAKASONE. Senator, certainly the entire defense of our, you know, electrical system within our critical infrastructures is of great concern to me. I am aware that there has been reporting with regards to elements within—within our ICS and SCATA systems. That's something that should concern all of us.

Senator KING. Do you see part of your job at NSA as working with the private sector? Because this is not—it's not like there's an attack on an air base. There might be an attack on the financial system or on the electrical system in the Midwest. And it seems to me this is an area, it's sort of new territory, if you will, where there has to be a closer relationship between the private sector and government.

General NAKASONE. Senator, I certainly agree with you in terms of the new relationship. If we consider cyberspace, 90 percent of, you know, our critical infrastructure is held within the private sector.

Senator KING. Right.

General NAKASONE. Currently right now, you know, the work that DHS does in terms of informing the private sector in the critical infrastructure is critical for us. In terms of the future, you know, I would see that in looking at, you know, if we're understanding what's going on in the sector, obviously a rich dialogue has to occur between, you know, the National Security Agency and those that—that have this type of technology.

Senator KING. Does that dialogue exist today?

General NAKASONE. Senator, I would—I would have to defer on that. That's something that, given my current position in Army Cyber, I'm not sure.

Senator KING. But I take it if confirmed for this position, that dialogue is something you would seek to—to establish?

General NAKASONE. Senator, certainly a dialogue with industry, but I would also say a dialogue with, you know, our universities and academia, our dialogue with a partnership. I think those are all kind of components that you have to have if you are going to lead a place like the National Security Agency.

Senator KING. I'm changing the subject entirely in the few seconds I have left. I just heard a new term, "STEMorrhage." That's a hemorrhage of STEM people. And that that's something that is

occurring at the NSA. Is this something—how can we compete to retain and attract the strongest STEM talent, which is what we need, in competition with Silicon Valley or the private sector? And is this a priority that you see as important in your mission?

General NAKASONE. Senator, in terms of priorities if confirmed, I can't imagine a more important priority than talent. In terms of STEM, again I thank the committee for their support for, you know, future pay increases for STEM candidates within the National Security Agency.

The way that I would assess that we have to look at it is we have to begin with: What's the mission of the agency? Because for many, many years the agency has been able to recruit and train and retain the best in our Nation based upon the idea of being able to secure our Nation and being able to defend it. I think that still is an advantage that the agency has. I think that appeals to people.

And I would also offer that NSA is a place where technological advances in innovation occur all the time. And I think that that is of great interest to our young people.

Senator KING. I hope and I understand that this will be a priority, because ultimately talent is the ultimate competitive advantage. And I commend you for your willingness to take on what is a very important challenge in our country. Thank you, General.

Chairman BURR. Senator Cotton.

Senator COTTON. Thank you, Mr. Chairman.

And thank you, General, for your appearance. Congratulations on your nomination. I'd like to discuss with you the threat posed to the U.S. national security by Chinese telecom companies like Huawei, ZTE, China Unicom, China Telecom. I believe this threat is grave.

I've introduced legislation that would prohibit the U.S. Government from using Huawei or ZTE or even companies that use them. I think there's a good chance we'll pass that into law this year.

Last month, at our Worldwide Threats Hearing, I asked all of the intelligence agency directors that appeared before us—DNI Coats, Director Wray, General Ashley, Director Cardillo, Admiral Rogers, Director Pompeo, Secretary-designate Pompeo—if they would use Huawei, ZTE, China Unicom, China Telecom products. They all said they would not. Would you use any products from those companies, General?

General NAKASONE. I would not, Senator.

Senator COTTON. Okay. You're a special case because you're about to be the director of the signals intelligence agency of our government. So would you recommend to any of your family or friends that are just normal private citizens, that they use products from those companies?

General NAKASONE. I would not, Senator.

Senator COTTON. Thank you for that.

President Trump two days ago, using the powers that he has under current law and from the CFIUS's recommendation, stopped the attempted takeover of Qualcomm by Broadcom. It's no secret that that's done in part because Qualcomm and Huawei are in a competition to establish the worldwide standards and protocols for the 5G network.

The intelligence community, though not a member of CFIUS, is an ex officio member. And on something like that, it would probably be assigned to the DNI who would task it out to, most likely, the NSA to give advice. Do you think CFIUS and the President made the right decision to stop the attempted takeover of Qualcomm by Broadcom?

General NAKASONE. So, Senator, I'm aware of the situation based upon what I've read in the public reports. I don't have any other background on this. But what I would say is our microelectronics industry is critical for us for the future. If you consider what 5G will bring to this Nation, 100 times speeds of what we're experiencing today, it's hard not to imagine the importance of ensuring that we have confidence in our microelectronics industry for the future.

Senator COTTON. Thank you.

I am somewhat concerned that some of our allies don't share our concerns about Huawei and ZTE. Can I ask you, if confirmed, that you'll consult with the Five Eyes partners and other partners, South Korea and Japan, to try to convey our government's concerns about Huawei and ZTE?

General NAKASONE. I certainly will, Senator.

Senator COTTON. And maybe if we could talk about that, if confirmed, at one of your early hearings. I know you just committed 90 days in to look at the dual hat issue. If maybe 90 days in we could talk about that in a classified setting would be fine.

A somewhat similar topic is the counterintelligence and security threats that could be posed by certain GPS-reliant devices, things like Fitbits and smartphones. There was a recent story in The Washington Post I suspect you saw, about soldiers using Fitbits around the world. Secretary Mattis, I thought wisely, ordered a review of DOD policies and procedures regarding these devices.

Senator Blumenthal and I also sent Secretary Mattis a letter asking that he include other devices, particularly Google and Android devices, as part of that review, because it appears that Google and Android send quite a bit of information from their devices back home to the mothership. That means they track very detailed user information and precise location in order to push people advertisements. So, for instance, if you drive past the same grocery store or department store every single day, pretty soon you are getting advertisements from those locations.

How would you view the privacy and counterintelligence threats posed by devices like these Fitbits and smartphones that are tracking locations, revealing patterns of life, and send them back to headquarters? Privacy for our private citizens, but counterintelligence for our government employees, and especially intelligence officers and military personnel?

General NAKASONE. Senator, I think you accurately describe the environment upon which we live today. This is commander's business with regards to, in the Army, our operational security. Ten, 15, 20 years ago, we were concerned about what we said on phones. Today, we're concerned about what our soldiers wear, where they're talking, where they are able to be monitored. And I think that this is indicative of how we have to approach the future, which is we

are technologically informed; we also have to be informed for our operational security as well.

Senator COTTON. Any thoughts on how we can balance the legitimate uses of those technologies? I mean, most soldiers are living on a limited budget, so it's valuable for them to have advertisements pushed to them saying, you know, when a restaurant is offering a special on the way home, or if a grocery store is having—has some coupons, and things like that. But obviously, these do pose a security risk. Any thoughts on how to balance those?

General NAKASONE. Senator, I believe you—you have to begin with just understanding what perhaps the threats are out there, and understanding, you know, when is it appropriate that civilians that are working in a place like the National Security Agency or military members within their own formations have their phones or are wearing Fitbits. Is there—are there places where they shouldn't have those things on? And, I think that that's, perhaps, the most important piece that we have to have is realization, and then an understanding of those operational security risks.

Senator COTTON. Thank you, General.

Chairman BURR. Senator Harris.

Senator HARRIS. Thank you.

And to follow-up on Senator Cotton's questions: Will you commit to coming back to our committee after doing an assessment of the vulnerabilities that are created by the use of these smart devices by our troops, and give us some suggestion about what might be a more appropriate policy?

General NAKASONE. Certainly—I'm sorry, Senator. I would welcome the opportunity to continue this dialogue on that.

Senator HARRIS. Okay. Thank you.

I'd like to talk with you about insider threats. According to the Office of the Director of National Intelligence, as of October of 2015 4.3 million Americans held security clearances. Some of the most damaging national security breaches in recent years, however, have not come from traditional spies, but insiders at our own agencies. Unfortunately, several of these incidents happened at NSA, and I am thinking three in particular that received a lot of attention and did a lot of damage. Have you studied what happened in those cases?

General NAKASONE. Senator, to date in my current role I have not studied. I would offer that I think what you point out here is very important, that we considered most of our threats from external actors. We thought that a foreign nation was, you know, our greatest threat. We have to reconsider that, particularly as we look at our networks, our data, our weapon systems. We have to have a whole spectrum of insider and, certainly, external threats as well.

Senator HARRIS. And will you commit to doing an assessment and reporting back to us on what additional steps might be taken to prevent that insider threat?

General NAKASONE. Senator, I do know that the NSA has undertaken a number of different initiatives, "Secure the Network" and "Secure the Enterprise." If confirmed, I will certainly commit to digging deep into that, understanding what has been done, what has been successful, what needs to be perhaps funded for the fu-

ture, and then continuing that dialogue with this committee, if that's okay.

Senator HARRIS. Yes. And have you had any experience dealing with this at Army Cyber Command?

General NAKASONE. So, Senator, in terms of experience, I would say that one of the things that we have been very, very vigilant about is just understanding the threats, again, to our network, our data and our weapons systems. I can't think of a specific example, but I will tell you that it is something that we are obviously trained on and think about very, very often.

Senator HARRIS. And I want to talk—there's been discussion with you already, but I'd like to get a little deeper into the issue of the talent drain issue and recruiting. There's a report that suggests that since 2015, the NSA has lost several hundred employees, including engineers and data scientists.

We know that we're going to be outpaced by the private sector in terms of salaries. So to your point, people who come to us to serve the public will do it because they actually care about public service and working on behalf of our government. But have you given any thought to how we might engage the private sector workforce—and I'm thinking of the folks of Silicon Valley—in creative ways that might include, for example, bringing people on who cannot join the IC full-time?

Have you thought about that and what would that look like? I think it would be challenging, but there must be some creative thoughts out there about we could engage folks, even if they don't come full-time.

General NAKASONE. Senator, I have thought about that. And, you know, I take example of what NSA has done to date with their own Point of Presence, which is an initiative to be in Silicon Valley and one of their early initiatives, even before DIUx. I think it's a very good example of how we need to think about the future.

You indicate one way that we might look at in bringing a larger population to our mission. I would offer, one of the things that I most admired about the agency is that they are looking at a very, very broad range of capabilities, people that have even disabilities that, you know, that need to be able to work, and have the infrastructure that will support that. I think that's tremendously important for us as we look at a broader supply, a broader talent base, that we need to be able to prosecute our mission.

Senator HARRIS. And I really appreciate that you mentioned the disabled community as part of the focus and what should be the focus about how we are thinking about the need to be more diverse in terms of our recruitment and retention policies. So, thank you for that.

And then election security. Admiral Rogers recently testified, and I'm going to quote, "What I see on the Cyber Command side leads me to believe that if we don't change the dynamic here, that this is going to continue and 2016 won't be viewed as isolated." And then he went on to add, "We're taking steps, but we're probably not doing enough" on the issue of election security. Do you agree with that statement?

General NAKASONE. Senator, in my current role I do not have, obviously, the background of what Admiral Rogers was speaking to.

That's not part of my current responsibilities, but certainly, if confirmed, one of the most important things that I would face in the new term, to learn more about this and make that assessment.

Senator HARRIS. And I'd ask that you would make that a priority as soon as you are confirmed, expecting that you will be, because obviously folks are starting to vote now and the 2018 election is upon us. So, thank you for that.

Chairman BURR. Thank you, Senator.

General, we have exhausted the members that have questions here today. I have asked members to submit questions for the record by the end of business today. And I would once again say to designees, please try to meet that deadline.

I would also say to you, if you would respond to those questions for the record as timely a manner as you can it would benefit us greatly to set the schedule for moving your nomination out of the committee and falling within the time frame that we're working with with the Senate Defense Committee.

It strikes me you've been nominated at a very pivotal time where technology, as the Vice Chairman pointed out, is changing annually the same way technology used to change literally decade by decade. And I think this is a tremendous opportunity and it is a tremendous challenge. I think you're the right person at the right time.

And I think your ability to understand whether that technological change is an asset to you or a liability—and I think that was in the crux of Senator Wyden's question about encryption, and it sort of depends on which window you're looking at in the same room.

It's tough for me to admit that you're the right person at the right time because I never thought that I would say that about somebody that had—a soldier that had never rotated through a North Carolina facility.

General NAKASONE. Sorry, Mr. Chairman.

[Laughter.]

Chairman BURR. But I do want to say to you that we're grateful for your service to the country. We look forward to your leadership at NSA. The relationship between this committee and that agency has never been better than it is right now, and I think that that's because it's been earned on both sides, the agency and the committee.

The agency has provided us an unprecedented access to its products as we've worked for the last 14 months through a very difficult investigation, which is distinctly different from the oversight role, traditional oversight role of the committee. And I would ask you, as long as that investigation continues, that it's important on your end that you distinguish the request for the investigative portion from the oversight, ongoing oversight and real-time oversight of the committee, because it will require us to see products that we wouldn't historically ask for and, if we did, we would probably be refused.

But it is essential for this committee to do a thorough and complete review of what has happened to our election system, what has happened from a standpoint of phishing operations—I'm not telling you anything that you don't know, given your current role—that has been exploited, that will only get worse in the future. Our abil-

ity to understand that and to not only enhance our defensive capabilities, but to begin, as the Vice Chairman says frequently, to form a strategic outline of options that we have, both defensive and offensive, is absolutely important.

So we put a tremendous amount of emphasis on our ability to get this right, and in large measure that's because of the access that the NSA has provided us. And I'm sure that under your leadership that will continue.

General, we're proud of you. But, more importantly, we're proud of the men and women that every day go to the National Security Agency, many of them without any public acknowledgement that they work there. It's not the prettiest campus, as you know. It's not in the easiest place to get to in Northern Virginia and Southern Maryland.

But they go there and they sacrifice salary for a commitment to their country. And they provide the foundation for the protection and security of the American people. We can't say enough times to them: "Thank you for what you do."

We are here as a tool for you, for your successful leadership at the NSA that we know will happen. And I hope you will call on us anytime we can enhance that role as Director of the National Security Agency.

With that, this hearing is adjourned.

[Whereupon, at 11:07 a.m., the hearing was adjourned.]

Supplemental Material

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

QUESTIONNAIRE FOR COMPLETION BY PRESIDENTIAL NOMINEES

SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE

QUESTIONNAIRE FOR COMPLETION BY PRESIDENTIAL NOMINEES

PART A - BIOGRAPHICAL INFORMATION

1. FULL NAME: Paul M. Nakasone
   OTHER NAMES USED: N/A

2. DATE AND PLACE OF BIRTH:
   19 November 1963, Saint Paul, MN
   CITIZENSHIP: US

3. MARITAL STATUS: Married

4. SPOUSE'S NAME: Susan S. Nakasone

5. SPOUSE'S MAIDEN NAME IF APPLICABLE: Sternberg

6. NAMES AND AGES OF CHILDREN:

NAME	AGE

INFORMATION REDACTED

7. EDUCATION SINCE HIGH SCHOOL:

INSTITUTION	DATES ATTENDED	DEGREE RECEIVED	DATE OF DEGREE
Saint John's University	Sep '82-Jun '86	Bachelor Of Arts	May '86
Univ Of Southern Calif	May '87-May '89	Master Of Science In Systems Management	May '89
Defense Intelligence College	Aug '90-Jun '91	Master Of Science In Strategic Intelligence	Jun '92
Army War College	Aug '06-Jun '07	Master Of Strategic Studies	Jun '07

8. EMPLOYMENT RECORD (LIST ALL POSITIONS HELD SINCE COLLEGE, INCLUDING MILITARY SERVICE. INDICATE NAME OF EMPLOYER, POSITION, TITLE OR DESCRIPTION, LOCATION, AND DATES OF EMPLOYMENT).

EMPLOYER	POSITION/TITLE	LOCATION	DATES
U.S. Army	Commanding General, United States Army Cyber Command	Fort Belvoir, Virginia	Oct 16 - Present
U.S. Army	Commander, Cyber National Mission Force, United States Cyber Command	Fort Meade, Maryland	May 14 - Oct 16
U.S. Army	Deputy Commanding General (Operations), United States Army Cyber Command	Fort Belvoir, Virginia	Aug 13 - May 14
U.S. Army	Director, Information Dominance Center, later Deputy Chief of Staff, Intelligence, CJ-2, International Security Assistance Force Joint Command, OPERATION ENDURING FREEDOM	Afghanistan	Jun 12 - Jun 13
U.S. Army	Deputy Director for Information and Cyberspace Policy, later Deputy Director for Trans-Regional Policy, J-5, Joint Staff	Washington, DC	Jun 11 - Jun 12
U.S. Army	Executive Assistant to the Commander, United States Cyber Command	Fort Meade, Maryland	Jun 10 - Jun 11
U.S. Army	Commander, Meade Operations Center, National Security Agency/Central Security Service	Fort Meade, Maryland	Jun 07 - Jun 10
U.S. Army	Student, United States Army War College	Carlisle Barracks, Pennsylvania	Aug 06 - Jun 07
U.S. Army	Chief, Intelligence Plans Division, Office of the Deputy Chief of Staff for Strategy, Plans and Assessment, Multi-National Force-Iraq, OPERATION IRAQI FREEDOM	Iraq	Jul 05 - Jun 06
U.S. Army	Assistant Chief of Staff, G-2, 24th Infantry Division (Mechanized)	Fort Riley, Kansas	Jun 04 - May 05
U.S. Army	Commander, 206th Military Intelligence Battalion, 116th Military Intelligence Group	Fort Gordon, Georgia	Jun 02 - Jun 04
U.S. Army	Intelligence Planner, J-2, Joint Staff (Defense Intelligence Agency)	Washington, DC	Jul 99 - May 02
U.S. Army	Plans Officer, later Operations Officer, 501st Military Intelligence Brigade, Eighth United States Army	Republic of Korea	Jul 97 - Jun 99
U.S. Army	Student, United States Army Command and General Staff College	Fort Leavenworth, Kansas	Aug 96 - Jun 97
U.S. Army	Assignments Officer, Military Intelligence Branch, United States Total Army Personnel Command	Alexandria, Virginia	Feb 94 - Jun 96
U.S. Army	Commander, A Company, 102d Military Intelligence Battalion, 2d Infantry Division, Eighth United States Army	Republic of Korea	Jan 93 - Jan 94
U.S. Army	Assistant Operations Officer, 102d Military Intelligence Battalion, 2d Infantry Division, Eighth United States Army	Republic of Korea	Jul 92 - Jan 93
U.S. Army	Plans and Operations Officer, Plans and Targets Branch, CJ-2, Eighth United States Army	Republic of Korea	Oct 91 - Jul 92
U.S. Army	Student, Postgraduate Intelligence Program, Defense Intelligence College	Washington, DC	Aug 90 - Jun 91

EMPLOYER	POSITION/TITLE	LOCATION	DATES
U.S. Army	Student, Military Intelligence Officer Advanced Course, United States Army Military Intelligence Center and School	Fort Huachuca, Arizona	May 90 - Jul 90
U.S. Army	Platoon Leader, later Executive Officer, A Company, 104th Military Intelligence Battalion, 4th Infantry Division (Mechanized)	Fort Carson, Colorado	Apr 89 - Apr 90
U.S. Army	Intelligence Officer, 1st Battalion, 8th Infantry, 4th Infantry Division (Mechanized)	Fort Carson, Colorado	Dec 87 - Apr 89
U.S. Army	Assistant Intelligence Officer, 3d Brigade, 4th Infantry Division (Mechanized)	Fort Carson, Colorado	Mar 87 - Dec 87

9. GOVERNMENT EXPERIENCE (INDICATE EXPERIENCE IN OR ASSOCIATION WITH FEDERAL, STATE, OR LOCAL GOVERNMENTS, INCLUDING ADVISORY, CONSULTATIVE, HONORARY, OR OTHER PART-TIME SERVICE OR POSITION. DO NOT REPEAT INFORMATION ALREADY PROVIDED IN QUESTION 8).

   None

10. INDICATE ANY SPECIALIZED INTELLIGENCE OR NATIONAL SECURITY EXPERTISE YOU HAVE ACQUIRED HAVING SERVED IN THE POSITIONS DESCRIBED IN QUESTIONS 8 AND/OR 9.

    2011 Service on Joint Chiefs of Staff; Regularly attended National Security Council meetings

    2012 Director of Intelligence, IJC, Afghanistan; Intelligence Senior for US and Coalition Nations supporting combat operations in Afghanistan

11. HONORS AND AWARDS (PROVIDE INFORMATION ON SCHOLARSHIPS, FELLOWSHIPS, HONORARY DEGREES, MILITARY DECORATIONS, CIVILIAN SERVICE CITATIONS, OR ANY OTHER SPECIAL RECOGNITION FOR OUTSTANDING PERFORMANCE OR ACHIEVEMENT).

    Distinguished Service Medal
    Defense Superior Service Medal (with 3 Bronze Oak Leaf Clusters)
    Legion of Merit
    Bronze Star Medal
    Defense Meritorious Service Medal (with 1 Bronze Oak Leaf Cluster)
    Meritorious Service Medal (with 4 Bronze Oak Leaf Clusters)
    Army Commendation Medal
    Joint Service Achievement Medal (with 1 Bronze Oak Leaf Cluster)
    Army Achievement Medal (with 4 Bronze Oak Leaf Clusters)
    Combat Action Badge
    Joint Chiefs of Staff Identification Badge

12. ORGANIZATIONAL AFFILIATIONS (LIST MEMBERSHIPS IN AND OFFICES HELD WITHIN THE LAST TEN YEARS IN ANY PROFESSIONAL, CIVIC, FRATERNAL, BUSINESS, SCHOLARLY, CULTURAL, CHARITABLE, OR OTHER SIMILAR ORGANIZATIONS).

ORGANIZATION	OFFICE HELD	DATES
Japanese American Veterans Association	None	Apr 2011-Present

13. PUBLISHED WRITINGS AND SPEECHES (LIST THE TITLES, PUBLISHERS, BLOGS AND PUBLICATION DATES OF ANY BOOKS, ARTICLES, REPORTS, OR OTHER PUBLISHED MATERIALS YOU HAVE AUTHORED. ALSO LIST ANY PUBLIC SPEECHES OR REMARKS YOU HAVE MADE WITHIN THE LAST TEN YEARS FOR WHICH THERE IS A TEXT, TRANSCRIPT, OR VIDEO). IF ASKED, WILL YOU PROVIDE A COPY OF EACH REQUESTED PUBLICATION, TEXT, TRANSCRIPT, OR VIDEO?

EVENT	LOCATION	DATE
PANELIST: AFCEA Cyber Education Resource & Training symposium – https://www.afcea.org/site/certs18-archive	Augusta, GA	January 17, 2018
KEYNOTE SPEAKER: Association of the United States Army, Hot Topics: Cyber - https://www.youtube.com/watch?v=hMqszDCJHQc	Arlington, VA	December 13, 2017
KEYNOTE SPEAKER: University of Pittsburgh academic outreach	Pittsburgh, PA	November 15, 2017
PANELIST: ISRC2 Battle Management Conference	Bethesda, MD	November 7, 2017
KEYNOTE SPEAKER: Army Cyber Institute CyCon – https://www.youtube.com/watch?v=hMqszDCJHQc	Washington, DC	November 7, 2017
KEYNOTE SPEAKER - Cyber Georgia https://echo360.org/media/c145e6f6-cb8d-4c62-a096-8c5906f9670e/public	Augusta, GA	October 13, 2017
PANELIST: Association of the United States Army, Contemporary Military Forum, Cyber Workforce https://www.dvidshub.net/video/558976/ausa-2017-cmf-9-new-kind-force-new-fighting-domain-cyber-talent-management	Washington, DC	October 12, 2017
MEDIA INTERVIEW: Cyber Support to Tactical Units	Washington, DC	October 12, 2017
KEYNOTE SPEAKER: Hawaii Future Focus Conference	Honolulu, HI	October 4, 2017
PANELIST: Institute for the Study of War conference -	Washington, DC	September 25, 2017
PANELIST: Intelligence and National Security Summit -	Washington, DC	September 6, 2017
PANELIST: US Military Academy dinner	New York, NY	September 5, 2017
KEYNOTE SPEAKER: Task Force Echo launch ceremony https://www.dvidshub.net/video/544338/task-force-echo-transfer-authority-ceremony	Ft. Meade, MD	August 15, 2017
KEYNOTE SPEAKER: AFCEA TechNet https://www.youtube.com/watch?v= WJmfhuvBaI	Augusta, GA	August 8, 2017
KEYNOTE SPEAKER: Defense One Tech Summit – http://www.defenseone.com/feature/defense-one-tech-summit-2017-livestream/	Washington, DC	July 13, 2017
KEYNOTE SPEAKER: National Cyber Summit –	Huntsville, AL	June 6, 2017
KEYNOTE SPEAKER: Civilian Aides to the Secretary of the Army, National Summit	Ft. Bragg, NC	June 5, 2017
KEYNOTE SPEAKER: Asian-Pacific Islander Month –	Ft. Belvoir, VA	May 31, 2017
TESTIMONY: Senate Armed Services, Cyber Subcommittee https://www.youtube.com/watch?v=6CR6l_0T2-c	Washington, DC	May 23, 2017

EVENT	LOCATION	DATE
KEYNOTE SPEAKER: Billington International Cyber Summit	Washington, DC	March 30, 2017
PUBLICATION: Cyber Defense Review – Article co-author, "Cyberspace in Multi-Domain Battle" http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1134630/cyberspace-in-multi-domain-battle/	Publication	March 28, 2017
PANELIST: AFCEA OffSet Symposium	San Francisco, CA	February 15, 2017
MEDIA INTERVIEW: Government Matters TV; https://www.youtube.com/watch?v=--QwJhCIHXo	San Francisco, CA	February 14, 2017
PANELIST: BENS Dinner Event	San Francisco, CA	February 14, 2017
PANELIST: RSA Public Sector Day	San Francisco, CA	February 13, 2017
KEYNOTE SPEAKER: Groundbreaking Ceremony Army Cyber Headquarters - https://www.youtube.com/watch?v=FNzJ4i7ZFsg&t=3s	Ft. Gordon, GA	November 29, 2016
INTRODUCTORY SPEAKER: Association of the United States Army, Hot Topics: Cyber https://www.youtube.com/watch?v=y-Y3STh4wWk&t=364s	Arlington, VA	November 15, 2016
PANELIST: AUSA Hot Topics, Army Networks, Readiness and the Joint Information Environment https://www.youtube.com/watch?v=qnpHXSil0CA	Arlington, VA	July 14, 2016
PANELIST: Association of the United States Army Annual Meeting: Army Cyber Today and Tomorrow; https://www.youtube.com/watch?v=oDOiBiey4cU	Washington, DC	October 14, 2015
PANELIST: Center for Strategic and International Studies, The Role of the U.S. Military in Cyberspace https://www.youtube.com/watch?v=qHKE4Remyow	Washington, DC	October 13, 2015
PANELIST: Army Cyber Institute Leadership Discussion, Leading and Winning in a Complex World	New York, NY	September 30, 2015
CLOSING REMARKS; Army Cyber Talks 2014 - https://www.youtube.com/watch?v=uRUgwQKZ60Q	West Point, NY	January 25, 2015
MEDIA INTERVIEW – Reuters; https://in.reuters.com/video/2014/05/13/army-adding-cyber-armor-against-inside-t?videoId=312922396	Washington, DC	May 13, 2014
MODERATOR: International Cyber Collaboration Panel at the 2011 Cyber and Space Symposium https://www.youtube.com/watch?v=0OPAT7eHS8o	Omaha, NE	November 16, 2011
US Army War College Strategy Research Project, A Strategy for the End Game in Iraq, available at http://www.dtic.mil/get-tr-doc/pdf?AD=ADA468944	Publication	March 2007

This list reflects my best efforts to identify all published writings and speeches. As a senior officer, I frequently make public remarks, at times unscheduled, and these remarks may not be reflected in my records.

If asked, I will provide a copy of each requested publication, text, transcript, or video.

PART B - QUALIFICATIONS

14. QUALIFICATIONS (DESCRIBE WHY YOU BELIEVE YOU ARE QUALIFIED TO SERVE AS THE DIRECTOR OF THE NATIONAL SECURITY AGENCY).

I am a career intelligence officer. For over three decades, I have served in intelligence positions across Joint and Army forces in peace and war. I understand how to produce timely, accurate, and valued intelligence, and what consumers demand of our intelligence products. During all of these tours I have benefitted from the intelligence produced by the National Security Agency.

Besides serving as a senior intelligence officer, I have also led and commanded large organizations, both Joint and Army, at every level of our military. I understand the importance of strategic vision, the criticality of placing people first, and the power of a mission centered on the defense of our Nation.

My service has also included formative assignments with the Joint Staff, Multi-National Forces Iraq, US Forces Afghanistan, and US Cyber Command. During these tours I have served with and under some of the finest civilian and military leaders our nation has produced. These experiences have afforded me insight into leadership at the strategic, operational, and tactical levels, with broadening exposure to the interagency, coalition partners, commercial industry, and academia.

Finally, I have served within the National Security Agency on three separate occasions. On each of these tours, I have admired the talent, the technological and innovative spirit, and the tradecraft of this world-class intelligence organization. If confirmed, I believe my previous intelligence experience, my ability to lead large organizations, and my familiarity with the NSA mission and its people would serve as a firm foundation upon which to serve as its next Director.

PART C - POLITICAL AND FOREIGN AFFILIATIONS

15. POLITICAL ACTIVITIES (LIST ANY MEMBERSHIPS OR OFFICES HELD IN OR FINANCIAL CONTRIBUTIONS OR SERVICES RENDERED TO, ANY POLITICAL PARTY, ELECTION COMMITTEE, POLITICAL ACTION COMMITTEE, OR INDIVIDUAL CANDIDATE DURING THE LAST TEN YEARS).

None

16. CANDIDACY FOR PUBLIC OFFICE (FURNISH DETAILS OF ANY CANDIDACY FOR ELECTIVE PUBLIC OFFICE).

None

17. FOREIGN AFFILIATIONS

(NOTE: QUESTIONS 17A AND B ARE NOT LIMITED TO RELATIONSHIPS REQUIRING REGISTRATION UNDER THE FOREIGN AGENTS REGISTRATION ACT. QUESTIONS 17A, B, AND C DO NOT CALL FOR A POSITIVE RESPONSE IF THE REPRESENTATION OR TRANSACTION WAS AUTHORIZED BY THE UNITED STATES GOVERNMENT IN CONNECTION WITH YOUR OR YOUR SPOUSE'S EMPLOYMENT IN GOVERNMENT SERVICE.)

A. HAVE YOU OR YOUR SPOUSE EVER REPRESENTED IN ANY CAPACITY (E.G. EMPLOYEE, ATTORNEY, OR POLITICAL/BUSINESS CONSULTANT), WITH OR WITHOUT COMPENSATION, A FOREIGN GOVERNMENT OR AN ENTITY CONTROLLED BY A FOREIGN GOVERNMENT? IF SO, PLEASE FULLY DESCRIBE SUCH RELATIONSHIP.

No

B. HAVE ANY OF YOUR OR YOUR SPOUSE'S ASSOCIATES REPRESENTED, IN ANY CAPACITY, WITH OR WITHOUT COMPENSATION, A FOREIGN GOVERNMENT OR AN ENTITY CONTROLLED BY A FOREIGN GOVERNMENT? IF SO, PLEASE FULLY DESCRIBE SUCH RELATIONSHIP.

No

C. DURING THE PAST TEN YEARS, HAVE YOU OR YOUR SPOUSE RECEIVED ANY COMPENSATION FROM, OR BEEN INVOLVED IN ANY FINANCIAL OR BUSINESS TRANSACTIONS WITH, A FOREIGN GOVERNMENT OR ANY ENTITY CONTROLLED BY A FOREIGN GOVERNMENT? IF SO, PLEASE PROVIDE DETAILS.

No

D. HAVE YOU OR YOUR SPOUSE EVER REGISTERED UNDER THE FOREIGN AGENTS REGISTRATION ACT? IF SO, PLEASE PROVIDE DETAILS.

No

18. DESCRIBE ANY LOBBYING ACTIVITY DURING THE PAST TEN YEARS, OTHER THAN IN AN OFFICIAL U.S. GOVERNMENT CAPACITY, IN WHICH YOU OR YOUR SPOUSE HAVE ENGAGED FOR THE PURPOSE OF DIRECTLY OR INDIRECTLY INFLUENCING THE PASSAGE, DEFEAT, OR MODIFICATION OF FEDERAL LEGISLATION, OR FOR THE PURPOSE OF AFFECTING THE ADMINISTRATION AND EXECUTION OF FEDERAL LAW OR PUBLIC POLICY.

None

PART D - FINANCIAL DISCLOSURE AND CONFLICT OF INTEREST

19. DESCRIBE ANY EMPLOYMENT, BUSINESS RELATIONSHIP, FINANCIAL TRANSACTION, INVESTMENT, ASSOCIATION, OR ACTIVITY (INCLUDING, BUT NOT LIMITED TO, DEALINGS WITH THE FEDERAL GOVERNMENT ON YOUR OWN BEHALF OR ON BEHALF OF A CLIENT), WHICH COULD CREATE, OR APPEAR TO CREATE, A CONFLICT OF INTEREST IN THE POSITION TO WHICH YOU HAVE BEEN NOMINATED.

None

20. DO YOU INTEND TO SEVER ALL BUSINESS CONNECTIONS WITH YOUR PRESENT EMPLOYERS, FIRMS, BUSINESS ASSOCIATES AND/OR PARTNERSHIPS, OR OTHER ORGANIZATIONS IN THE EVENT THAT YOU ARE CONFIRMED BY THE SENATE? IF NOT, PLEASEEXPLAIN.

Yes

21. DESCRIBE THE FINANCIAL ARRANGEMENTS YOU HAVE MADE OR PLAN TO MAKE, IF YOU ARE CONFIRMED, IN CONNECTION WITH SEVERANCE FROM YOUR CURRENT POSITION. PLEASE INCLUDE SEVERANCE PAY, PENSION RIGHTS, STOCK OPTIONS, DEFERRED INCOME ARRANGEMENTS, AND ANY AND ALL COMPENSATION THAT WILL OR MIGHT BE RECEIVED IN THE FUTURE AS A RESULT OF YOUR CURRENT BUSINESS OR PROFESSIONAL RELATIONSHIPS.

None

22. DO YOU HAVE ANY PLANS, COMMITMENTS, OR AGREEMENTS TO PURSUE OUTSIDE EMPLOYMENT, WITH OR WITHOUT COMPENSATION, DURING YOUR SERVICE WITH THE GOVERNMENT? IF SO, PLEASE PROVIDE DETAILS.

No.

23. AS FAR AS CAN BE FORESEEN, STATE YOUR PLANS AFTER COMPLETING GOVERNMENT SERVICE. PLEASE SPECIFICALLY DESCRIBE ANY AGREEMENTS OR UNDERSTANDINGS, WRITTEN OR UNWRITTEN, CONCERNING EMPLOYMENT AFTER LEAVING GOVERNMENT SERVICE. IN PARTICULAR, DESCRIBE ANY AGREEMENTS, UNDERSTANDINGS, OR OPTIONS TO RETURN TO YOUR CURRENT POSITION.

Upon completion of my military service, I intend to retire, but have no current plans nor have I entered into any written or unwritten agreements or understandings, concerning employment after leaving government service.

24. IF YOU ARE PRESENTLY IN GOVERNMENT SERVICE, DURING THE PAST FIVE YEARS OF SUCH SERVICE, HAVE YOU RECEIVED FROM A PERSON OUTSIDE OF GOVERNMENT AN OFFER OR EXPRESSION OF INTEREST TO EMPLOY YOUR SERVICES AFTER YOU LEAVE GOVERNMENT SERVICE? IF YES, PLEASE PROVIDE DETAILS.

No

25. IS YOUR SPOUSE EMPLOYED? IF YES AND THE NATURE OF THIS EMPLOYMENT IS RELATED IN ANY WAY TO THE POSITION FOR WHICH YOU ARE SEEKING CONFIRMATION, PLEASE INDICATE YOUR SPOUSE'S EMPLOYER, THE POSITION, AND THE LENGTH OF TIME THE POSITION HAS BEEN HELD. IF YOUR SPOUSE'S EMPLOYMENT IS NOT RELATED TO THE POSITION TO WHICH YOU HAVE BEEN NOMINATED, PLEASE SO STATE.

No

26. LIST BELOW ALL CORPORATIONS, PARTNERSHIPS, FOUNDATIONS, TRUSTS, OR OTHER ENTITIES TOWARD WHICH YOU OR YOUR SPOUSE HAVE FIDUCIARY OBLIGATIONS OR IN WHICH YOU OR YOUR SPOUSE HAVE HELD DIRECTORSHIPS OR OTHER POSITIONS OF TRUST DURING THE PAST FIVE YEARS.

NAME OF ENTITY	POSITION	DATES HELD	SELF OR SPOUSE

None

27. LIST ALL GIFTS EXCEEDING $100 IN VALUE RECEIVED DURING THE PAST FIVE YEARS BY YOU, YOUR SPOUSE, OR YOUR DEPENDENTS. (NOTE: GIFTS RECEIVED FROM RELATIVES AND GIFTS GIVEN TO YOUR SPOUSE OR DEPENDENT NEED NOT BE INCLUDED UNLESS THE GIFT WAS GIVEN WITH YOUR KNOWLEDGE AND ACQUIESCENCE AND YOU HAD REASON TO BELIEVE THE GIFT WAS GIVEN BECAUSE OF YOUR OFFICIAL POSITION.)

None

28. LIST ALL SECURITIES, REAL PROPERTY, PARTNERSHIP INTERESTS, OR OTHER INVESTMENTS OR RECEIVABLES WITH A CURRENT MARKET VALUE (OR, IF MARKET VALUE IS NOT ASCERTAINABLE, ESTIMATED CURRENT FAIR VALUE) IN EXCESS OF $1,000. (NOTE: THE INFORMATION PROVIDED IN RESPONSE TO SCHEDULE A OF THE DISCLOSURE FORMS OF THE OFFICE OF GOVERNMENT ETHICS MAY BE INCORPORATED BY REFERENCE, PROVIDED THAT CURRENT VALUATIONS ARE USED.)

DESCRIPTION OF PROPERTY	VALUE	METHOD OF VALUATION

See section 6 of attached executive branch personnel public financial disclosure report (OGE Form 278e)

29. LIST ALL LOANS OR OTHER INDEBTEDNESS (INCLUDING ANY CONTINGENT LIABILITIES) IN EXCESS OF $10,000. EXCLUDE A MORTGAGE ON YOUR PERSONAL RESIDENCE UNLESS IT IS RENTED OUT, AND LOANS SECURED BY AUTOMOBILES, HOUSEHOLD FURNITURE, OR APPLIANCES. (NOTE: THE INFORMATION PROVIDED IN RESPONSE TO SCHEDULE C OF THE DISCLOSURE FORM OF THE OFFICE OF GOVERNMENT ETHICS MAY BE INCORPORATED BY REFERENCE, PROVIDED THAT CONTINGENT LIABILITIES ARE ALSO INCLUDED.)

NATURE OF OBLIGATION	NAME OF OBLIGEE	AMOUNT

See section 8 of attached executive branch personnel public financial disclosure report (OGE Form 278e)

ARE YOU OR YOUR SPOUSE NOW IN DEFAULT ON ANY LOAN, DEBT, OR OTHER FINANCIAL OBLIGATION? HAVE YOU OR YOUR SPOUSE BEEN IN DEFAULT ON ANY LOAN, DEBT, OR OTHER FINANCIAL OBLIGATION IN THE PAST TEN YEARS? HAVE YOU OR YOUR SPOUSE EVER BEEN REFUSED CREDIT OR HAD A LOAN APPLICATION DENIED? IF THE ANSWER TO ANY OF THESE QUESTIONS IS YES, PLEASE PROVIDE DETAILS.

No

30. LIST THE SPECIFIC SOURCES AND AMOUNTS OF ALL INCOME RECEIVED DURING THE LAST FIVE YEARS, INCLUDING ALL SALARIES, FEES, DIVIDENDS, INTEREST, GIFTS, RENTS, ROYALTIES, PATENTS, HONORARIA, AND OTHER ITEMS EXCEEDING $200. (COPIES OF U.S. INCOME TAX RETURNS FOR THESE YEARS MAY BE SUBSTITUTED HERE, BUT THEIR SUBMISSION IS NOT REQUIRED.)

INFORMATION REDACTED

31. IF ASKED, WILL YOU PROVIDE THE COMMITTEE WITH COPIES OF YOUR AND YOUR SPOUSE'S FEDERAL INCOME TAX RETURNS FOR THE PAST THREE YEARS?

Yes

32. LIST ALL JURISDICTIONS IN WHICH YOU AND YOUR SPOUSE FILE ANNUAL INCOME TAX RETURNS.

Federal, Virginia

33. HAVE YOUR FEDERAL OR STATE TAX RETURNS BEEN THE SUBJECT OF AN AUDIT, INVESTIGATION, OR INQUIRY AT ANY TIME? IF SO, PLEASE PROVIDE DETAILS, INCLUDING THE RESULT OF ANY SUCH PROCEEDING.

No

34. IF YOU ARE AN ATTORNEY, ACCOUNTANT, OR OTHER PROFESSIONAL, PLEASE LIST ALL CLIENTS AND CUSTOMERS WHOM YOU BILLED MORE THAN $200 WORTH OF SERVICES DURING THE PAST FIVE YEARS. ALSO, LIST ALL JURISDICTIONS IN WHICH YOU ARE LICENSED TO PRACTICE.

N/A

35. DO YOU INTEND TO PLACE YOUR FINANCIAL HOLDINGS AND THOSE OF YOUR SPOUSE AND DEPENDENT MEMBERS OF YOUR IMMEDIATE HOUSEHOLD IN A BLIND TRUST? IF YES, PLEASE FURNISH DETAILS. IF NO, DESCRIBE OTHER ARRANGEMENTS FOR AVOIDING ANY POTENTIAL CONFLICTS OF INTEREST.

No

36. IF APPLICABLE, LIST THE LAST THREE YEARS OF ANNUAL FINANCIAL DISCLOSURE REPORTS YOU HAVE BEEN REQUIRED TO FILE WITH YOUR AGENCY, DEPARTMENT, OR BRANCH OF GOVERNMENT. IF ASKED, WILL YOU PROVIDE A COPY OF THESE REPORTS?

2015, 2016, 2017

Yes

PART E - ETHICAL MATTERS

37. HAVE YOU EVER BEEN THE SUBJECT OF A DISCIPLINARY PROCEEDING OR CITED FOR A BREACH OF ETHICS OR UNPROFESSIONAL CONDUCT BY, OR BEEN THE SUBJECT OF A COMPLAINT TO, ANY COURT, ADMINISTRATIVE AGENCY, PROFESSIONAL ASSOCIATION, DISCIPLINARY COMMITTEE, OR OTHER PROFESSIONAL GROUP? IF SO, PLEASE PROVIDE DETAILS.

No

38. HAVE YOU EVER BEEN INVESTIGATED, HELD, ARRESTED, OR CHARGED BY ANY FEDERAL, STATE, OR OTHER LAW ENFORCEMENT AUTHORITY FOR VIOLATION OF ANY FEDERAL STATE, COUNTY, OR MUNICIPAL LAW, REGULATION, OR ORDINANCE, OTHER THAN A MINOR TRAFFIC OFFENSE, OR NAMED AS A DEFENDANT OR OTHERWISE IN ANY INDICTMENT OR INFORMATION RELATING TO SUCH VIOLATION? IF SO, PLEASE PROVIDE DETAILS.

No

39. HAVE YOU EVER BEEN CONVICTED OF OR ENTERED A PLEA OF GUILTY OR NOLO CONTENDERE TO ANY CRIMINAL VIOLATION OTHER THAN A MINOR TRAFFIC OFFENSE? IF SO, PLEASE PROVIDE DETAILS.

No

40. ARE YOU PRESENTLY OR HAVE YOU EVER BEEN A PARTY IN INTEREST IN ANY ADMINISTRATIVE AGENCY PROCEEDING OR CIVIL LITIGATION? IF SO, PLEASE PROVIDE DETAILS.

No

41. HAVE YOU BEEN INTERVIEWED OR ASKED TO SUPPLY ANY INFORMATION AS A WITNESS OR OTHERWISE IN CONNECTION WITH ANY CONGRESSIONAL INVESTIGATION, FEDERAL, OR STATE AGENCY PROCEEDING, GRAND JURY INVESTIGATION, OR CRIMINAL OR CIVIL LITIGATION IN THE PAST TEN YEARS? IF SO, PLEASE PROVIDE DETAILS.

No

42. HAS ANY BUSINESS OF WHICH YOU ARE OR WERE AN OFFICER, DIRECTOR, OR PARTNER BEEN A PARTY TO ANY ADMINISTRATIVE AGENCY PROCEEDING OR CRIMINAL OR CIVIL LITIGATION RELEVANT TO THE POSITION TO WHICH YOU HAVE BEEN NOMINATED? IF SO, PLEASE PROVIDE DETAILS. (WITH RESPECT TO A BUSINESS OF WHICH YOU ARE OR WERE AN OFFICER, YOU NEED ONLY CONSIDER PROCEEDINGS AND LITIGATION THAT OCCURRED WHILE YOU WERE AN OFFICER OF THAT BUSINESS.)

N/A

43. HAVE YOU EVER BEEN THE SUBJECT OF ANY INSPECTOR GENERAL INVESTIGATION? IF SO, PLEASE PROVIDE DETAILS.

No

PART F - SECURITY INFORMATION

44. HAVE YOU EVER BEEN DENIED ANY SECURITY CLEARANCE OR ACCESS TO CLASSIFIED INFORMATION FOR ANY REASON? IF YES, PLEASE EXPLAIN IN DETAIL.

No

45. HAVE YOU BEEN REQUIRED TO TAKE A POLYGRAPH EXAMINATION FOR ANY SECURITY CLEARANCE OR ACCESS TO CLASSIFIED INFORMATION? IF YES, PLEASE EXPLAIN.

2002—Assignment To Battalion Command, Fort Gordon, GA

2010—Assignment To Brigade Command, Fort Meade, MD

2016—Assignment To Army Cyber Command, Fort Belvoir, VA

46. HAVE YOU EVER REFUSED TO SUBMIT TO A POLYGRAPH EXAMINATION? IF YES, PLEASE EXPLAIN.

No

PART G - ADDITIONAL INFORMATION

47. DESCRIBE IN YOUR OWN WORDS THE CONCEPT OF CONGRESSIONAL OVERSIGHT OF U.S. INTELLIGENCE ACTIVITIES. IN PARTICULAR, CHARACTERIZE WHAT YOU BELIEVE TO BE THE OBLIGATIONS OF THE DIRECTOR OF THE NATIONAL SECURITY AGENCY AND THE INTELLIGENCE COMMITTEES OF THE CONGRESS, RESPECTIVELY, IN THE OVERSIGHT PROCESS

Congressional oversight refers to the responsibility of the legislative branch, rooted in the US Constitution, to monitor the activities of the executive branch. Oversight of the US Intelligence Community began in the late 1970s following the Church and Pike Commissions and the discovery of abuses of power and violations of law by several intelligence agencies. The role of the Director of the National Security Agency is first to ensure that the Agency's activities are consistent with the law and with applicable policies and procedures, and to hold individuals accountable as necessary. He is also responsible for informing Congress on Agency activities and, when necessary, must make himself available to answer questions and provide testimony at the request of Congress. Overall, the Director of the National Security Agency sets the tone for effective oversight throughout the entire enterprise by his words and his deeds. Congressional oversight involves supervision of the Intelligence Community and checking the potential for abuse of power. The intelligence committees exercise their oversight through legislative hearings, specialized investigations, nomination confirmation hearings, directed reviews and studies by congressional support agencies and staffs, and the power of the purse.

48. EXPLAIN YOUR UNDERSTANDING OF THE RESPONSIBILITIES OF THE DIRECTOR OF THE NATIONAL SECURITY AGENCY.

Under the authority, direction, and control of the Under Secretary of Defense for Intelligence (USD(I)), the Director of the National Security Agency is primarily responsible for ensuring the NSA successfully conducts two principal missions: signals intelligence (SIGINT) collection and information assurance protection. The collection of SIGINT, under Executive Order 12333, provides intelligence on America's adversaries. Through information assurance, conducted primarily under National Security Directive 42, the NSA protects America's vital national security information and systems from theft or damage by others.

The Director of the NSA also is the Chief of the Central Security Service, which includes the elements of the armed forces - Army, Navy, Air Force, Marine Corps, and Coast Guard - that perform cryptologic activities, including codemaking and codebreaking, along with the NSA.

The Director of the NSA also is dual-hatted as the Commander of US Cyber Command, currently a sub-unified command under US Strategic Command, responsible for planning, coordinating, integrating, synchronizing and conducting cyberspace operations.

AFFIRMATION

I, LIEUTENANT GENERAL PAUL M. NAKASONE, DO SWEAR THAT THE ANSWERS I HAVE PROVIDED TO THIS QUESTIONNAIRE ARE ACCURATE AND COMPLETE.

22 February 2018
(Date)

LTG NAKASONE SIGNATURE

NOTARY PUBLIC AUTHORIZED UNDER 10 U.S.C. 1044a

NOTARY SIGNATURE
(Notary)
IAN G. GORIS, COL, US ARMY

TO THE CHAIRMAN, SELECT COMMITTEE ON INTELLIGENCE:

In connection with my nomination to be the Director of the National Security Agency, I hereby express my willingness to respond to requests to appear and testify before any duly constituted committee of the Senate.

LTG NAKASONE SIGNATURE

Signature

Date: 22 February 2018

3/8/2018 3:20 PM

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

Additional Prehearing Questions for Lieutenant

General Paul M. Nakasone

Upon his nomination to be Director of the National Security Agency

Responsibilities of the Director of the National Security Agency

QUESTION 1: The role of Director of the National Security Agency (DIRNSA) has been performed differently depending on what the President has requested from the position. What do you see as your role as DIRNSA, if confirmed to this position? How do you expect it to be different than that of your predecessor?

The role of DIRNSA is to ensure the successful accomplishment of NSA's principal missions of protecting national security systems, and applying the capabilities of Signals Intelligence (SIGINT) to generate maximum insights in the areas of foreign intelligence and cyber security in the defense of our Nation and our friends and allies around the world within our Nation's legal framework and applicable policy guidance. The DIRNSA is equally responsible for the recruitment, training, and retention of a world-class workforce that underpins this mission.

If confirmed, I believe what may be unique to my tenure as DIRNSA is the level of challenge and complexity the future holds, including: increasing difficulties with the intelligence collection mission given rapid technological evolution; ubiquitous encryption; the growing capabilities of the private sector technology industry; ensuring continued network security from both external and internal threats; and the continuing challenge to retain an elite workforce given the many opportunities in the civilian sector.

QUESTION 2: The congressional intelligence committees have supported the Intelligence Community's (IC's) evaluation of dual-hatting the Commander of U.S. Cyber Command and DIRNSA positions. In the *Joint Explanatory Statement* accompanying the *Intelligence Authorization Act for Fiscal Year 2017* (P.L. 115- 31), the committees directed the IC to review and assess the potential impacts and effects. Specifically, the committees directed that the "organization of NSA should be examined to account for the evolution of its mission since its establishment, the current structure of the intelligence community, and the fact that the NSA is predominantly funded through the NIP." In all of the following, please include a discussion of the NSA's structure, budgetary procedures, and oversight responsibilities to Congress.

a. Which DIRNSA roles and responsibilities would be affected by a cessation of the dual-hat regime?

Any decision with respect to terminating the dual-hat leadership arrangement must be made in the best interests of the Nation and if directed, it must be conditions based – that is to say that processes and decisions which enable effective mutual collaboration and deconfliction are well established and operating. With that said, I believe terminating the dual hat leadership arrangement would have only minor effects on the DIRNSA's roles and responsibilities. The Director's primary responsibilities and NSA's mission will be largely unaffected. Given my

current assignment, I lack further details to discuss the NSA's budgetary structure, budgetary procedures and oversight responsibilities to Congress. If confirmed, this is an area that I will study further.

b. What in your view are the positive and negative aspects of a dual-hat regime? Please include assessments of structure, budgetary procedures, and oversight of NSA.

My experience is that the dual-hat arrangement has enabled the operationally close partnership between USCYBERCOM and the NSA, which benefits both in the accomplishment of their respective missions. Dual-hatting optimizes the integration and synchronization of SIGINT and cyberspace operations. It enables decision making that balances competing equities under the judgment of a single individual directly responsible for both organizations critical missions. If terminated, such decisions will require close organizational collaboration enabled by processes which build upon the operational integration achieved under the dual-hat arrangement, as well as close working relationships between the leaders of both organizations.

That said, I believe that any decision to maintain or terminate the dual-hat leadership arrangement must be conditions-based and in the best interests of the Nation. Each organization faces different challenges and has different mission goals – a distinction that risked blurring under dual-hatting and required continuous reinforcement of distinct mission focus for each organization. Given my current assignment, I lack further details to discuss the NSA's budgetary structure, budgetary procedures and oversight responsibilities to Congress. If confirmed, this is an area that I will study further.

c. What is your view on the dual-track supervision of NSA by the Secretary of Defense and the Director of National Intelligence?

NSA is both a Combat Support Agency and a DoD component within the Intelligence Community. Its mission is to help protect national security by providing both policy makers and military commanders with the intelligence information and cybersecurity insights they need. NSA has functioned effectively under this construct for decades, first, reporting to the Director of Central Intelligence and then to the Director of National Intelligence, once created. Dual-track supervision is appropriate and reflects the dual nature of NSA's mission.

QUESTION 3: Please describe the specific experiences you have had in your professional career that will enable you to serve effectively as the head of the NSA. In addition, what lessons have you drawn from the experiences of current and former DIRNSAs?

I am a career intelligence officer. For over three decades, I served in key intelligence positions across Joint and Army forces in peace and war. I understand how to produce timely,

accurate, and valued intelligence, and what consumers' demand of our intelligence products. My most recent intelligence assignment was as the Director of Intelligence, International Security Assistance Force Joint Command, Afghanistan.

My service has included formative assignments with the Joint Staff, Multi-National Forces Iraq, U.S. Forces Afghanistan, and USCYBERCOM. These experiences have afforded me significant insight into intelligence support at the strategic, operational, and tactical levels, with broadening exposure to the interagency, coalition partners, commercial industry, and academia.

Finally, I have served within the NSA on three separate occasions. This includes assignments to both Fort Gordon, Georgia and Fort Meade, Maryland. Over these multiple tours, I have developed a deep appreciation and strong commitment to the people and mission of the NSA.

QUESTION 4: If confirmed as DIRNSA, what steps will you take to improve the integration, coordination, and collaboration between NSA and the other IC agencies?

If confirmed, I will begin my analysis of the NSA's integration, coordination, and collaboration by looking inside the Agency. I would assess the degree of work being done by measuring the NSA's ability to enable SIGINT collection into other IC agency products, the placement of IC agency personnel within the NSA, and the degree of familiarity the workforce has for its IC counterparts.

I would then continue my assessment by seeking external views of the NSA's ability to integrate, coordinate, and collaborate within the other IC agencies. This feedback would come principally from the Director of National Intelligence and his staff, the Office of the Under Secretary of Defense for Intelligence, other members of the IC, and finally a discussion with our key product consumers—the DoD, the Interagency, Joint Staff, and Combatant Commands.

QUESTION 5: If confirmed as DIRNSA, how will you ensure that the tasking of NSA resources and personnel to support U.S. Cyber Command do not negatively impact NSA's ability to perform and fulfill core missions?

The dual hatted Director/Commander is supported by separate NSA and USCYBERCOM staffs. A series of interagency support agreements and memorandums of agreement are also in place to ensure the proper resource accounting occurs. I will make it my clear guidance that established business rules and processes designed to limit such impact are followed and enforced. If confirmed, part of my inherent responsibility under the dual-hat is to make such considerations a core part of my decision making and to be accountable such that negative impacts do not occur.

Keeping the Congressional Intelligence Committees Fully and Currently Informed

QUESTION 6: What is your understanding of DIRNSA's obligations under Title 50 of the National Security Act of 1947, including DIRNSA's obligation to appoint a Director of Compliance?

Title 50 contains numerous obligations for the DIRNSA. If confirmed, I will work with the NSA's Office of General Counsel to ensure full compliance with the law. This includes 50 U.S.C. 3602, which requires that there be a Director of Compliance for the Agency.

QUESTION 7: Please assess how well the NSA is working with Congress and, specifically, with the congressional intelligence committees.

It is my understanding that NSA works hard to keep Congress fully and currently informed. I am aware that NSA witnesses routinely testify before Congress and that the NSA personnel prepare briefings, papers, and notifications to Congress. I am also aware that at the recent hearing regarding the Intelligence Community's Worldwide Threat Assessment, the Chairman and Vice Chairman thanked the Intelligence Community for providing access to intelligence products, legal documents, and other materials necessary for Congress to carry out its oversight function. If confirmed, I look forward to continuing those efforts to keep Congress informed of NSA's activities.

a. What information should NSA share with Congress?

I believe NSA should not only be responsive to congressional requests, but should also proactively notify Congress of both successes and failures so that Congress can perform its important oversight role.

b. What, if any, information should NSA withhold from the congressional intelligence committees? Why?

NSA should not broadly withhold information from the congressional intelligence committees. In some cases, as has been my understanding of past practices, it may be best to provide details about NSA's most sensitive sources and methods only to select congressional intelligence leadership. To be clear, I do not believe the need to protect sensitive sources and methods overrides the NSA's obligation to inform Congress about its activities in a general sense. If confirmed, I will work with the congressional intelligence committees and strive to provide them with access to any materials required for their oversight of NSA operations.

QUESTION 8: Please describe your view of the NSA's obligation to respond to requests for information from Members of Congress.

If confirmed, I will work to ensure that my team understands Congress's important role overseeing NSA's activities. To fulfill that oversight function, NSA is obliged to provide

information, as appropriate, to the committees with jurisdiction over NSA's activities. I would work with Members to understand the outcome they are trying to achieve, and to help get the information that they need to fulfill this outcome.

QUESTION 9: Does NSA have a responsibility to correct the record, if it identifies occasions where inaccurate information has been provided to the congressional intelligence committees?

Yes. If confirmed, I will always be open with Congress and provide the best information available at the time, and if my subordinates or I need to correct the record, I will make sure that occurs.

QUESTION 10: This Committee is conducting an investigation into Russia's involvement in the 2016 U.S. election. If confirmed, will you support the Committee's oversight investigation and promptly provide any documents or briefings deemed necessary by the Committee?

Yes. I fully appreciate the significance of the Committee's investigation into Russia's involvement in the 2016 elections. Accordingly, if confirmed, I commit to continuing to support the Committee's need for documents and briefings relevant to the investigation in accordance with the procedures that have already been established.

Functions and Responsibilities of the National Security Agency

QUESTION 11: What do you consider to be the most important missions of the NSA?

Both of the NSA's principal missions, protecting national security systems and collecting foreign intelligence information, are paramount to the safety and security of our Nation. The two missions also go hand-in-hand. Collecting foreign intelligence information on our adversaries' attempts to penetrate our networks informs how best to protect national security systems, the security of which ensures (among other things) that adversaries remain unaware of our capabilities. Equally, the NSA's expertise in information assurance provides their operators insights into adversary systems, providing new opportunities for foreign intelligence collection. Together, these self-reinforcing missions allow the collection of foreign intelligence information critical to national security while protecting our Nation's own sensitive information.

QUESTION 12: How well do you think the NSA has performed recently in each of these missions?

I have limited awareness to assess this in my current assignment. There is always room for improvement, but generally, I think the NSA continues to provide an extraordinary service by generating high quality intelligence for our Nation's leaders and cybersecurity solutions to protect the most sensitive national security systems.

QUESTION 13: If confirmed, what missions do you expect to direct the NSA to prioritize over

others?

At a high level, it is clear that the Nation is at a growing risk from foreign malicious cyber actors, so I expect to emphasize increasing cyber capabilities in order to ensure NSA has awareness of foreign malicious cyber activities, including cyber attacks, and can provide policy makers with unique and timely foreign intelligence information. If confirmed, I will be in a better position to make fully informed assessments and establish clear priorities.

National Security Threats and Challenges Facing the Intelligence Community

QUESTION 14: What, in your view, are the current principal threats to national security most relevant to the NSA?

Cyber threats, weapons of mass destruction (WMD), and terrorist activities are the current principal threats to national security that are most relevant to the NSA. More specifically, growing near-peer foreign military powers powers, terrorist organizations, transnational criminal organizations, and other dangerous groups and individuals use cyber operations to achieve malign strategic objectives. North Korea, Russia, and China all have state efforts to modernize, develop, or acquire WMD, their delivery systems, or the underlying technologies. These efforts are a major threat to the United States and to our partners. Terrorist organizations also continue to expand their global presence, posing a persistent threat to the U.S. Homeland, its allies, and U.S. interests abroad.

QUESTION 15: In your opinion, how has the NSA performed in adjusting its policies, resource allocations, planning, training, and programs to address these threats?

Mindful that the NSA is a very large organization, I think the NSA has done an admirable job of adjusting to a rapidly changing threat landscape. The adjustment from a Cold War focus toward a foreign terrorism focus in the 1990s and 2000s was significant and challenging, but ultimately resulted in the NSA producing critical intelligence in the global war on terrorism. In the same manner, the Agency has made notable adjustments over the last decade to support success in the foreign cyber arena, while still maintaining its foreign counter-terrorism abilities. This is an area that I will be able to better assess, if confirmed.

QUESTION 16: What role do you see for the NSA, in particular, and the IC, as a whole, with respect to the ongoing challenge of ubiquitous encryption as it pertains to foreign intelligence?

The prevalence of encryption and the complexity of the math behind it has increased with the proliferation of computers, but the fundamental nature of encryption has not changed. Thus, the NSA's mission with regard to cryptology remains the same: develop robust encryption to protect national security systems and work with Intelligence Community partners and U.S. allies to ensure that the NSA has solutions to our adversaries' encryption and can continue to produce the foreign intelligence information that U.S. policymakers and military leaders rely upon. That said,

the Agency has previously stated publicly that the prevalence of encryption does create challenges and requires the NSA to focus on more resource-intensive ways to produce foreign intelligence information.

Foreign Intelligence Surveillance Act

QUESTION 17: The USA FREEDOM Act will sunset on December 15, 2019. What is your view on its reauthorization?

I am familiar with the authority and aware the statute sunsets in less than two years, but, if confirmed, I want to assess NSA's use of the authority before formulating an answer. I will work with my team to fully understand the USA FREEDOM Act's utility, resource requirements, compliance controls, and privacy protections. I believe it is important for the NSA to regularly evaluate its collection activities and optimize the legal authorities and the resources provided by Congress.

QUESTION 18: Has the transition from the NSA to the telecommunications companies regarding the metadata collection and retention of call detail records affected the IC's operational capabilities? If so, how?

If confirmed, I will seek to understand and assess this specific issue as part of the process of reviewing the USA FREEDOM Act.

Cybersecurity

QUESTION 19: As the nation's cyber infrastructure becomes increasingly susceptible to cyberattacks, can a single individual successfully execute both roles of DIRNSA and the head of U.S. Cyber Command?

I believe that General Alexander and Admiral Rogers have demonstrated that a single leader can successfully execute the roles of DIRNSA and Commander USCYBERCOM. The 2017 NDAA, Section 1642 placed a limitation on termination of the dual hat arrangement unless six conditions have been met. If confirmed, I will evaluate these conditions and provide my assessment to the Secretary of Defense and the Chairman of the Joint Chiefs of Staff, who must certify these conditions are met to ensure that termination does not pose risks to the operational effectiveness of either organization that are unacceptable to the national security interests of the United States. Ultimately, I believe that any decision must be conditions-based and in the best interests of the Nation.

QUESTION 20: What changes to the respective cybersecurity roles would occur if the dual-hat regime ceased to exist?

None; the cybersecurity roles of DIRNSA were not changed by the dual-hat arrangement, so terminating the dual hat arrangement would equally have no effect. Of course, there will be some practical consequences related to coordination that naturally flow from the new leadership arrangement, but these could be mitigated by mutual support agreements and other preparations. If confirmed, I would include this assessment in my recommendations to the Secretary of Defense, Chairman of the Joint Chiefs of Staff, and Director of National Intelligence.

QUESTION 21: What role do you see for the NSA in defensive cybersecurity policies or actions? What role do you see for NSA in supporting any U.S. Government offensive cybersecurity policies or actions?

DIRNSA is the National Manager for National Security Systems and in this capacity works closely with DoD to protect the Department of Defense information network (DODIN), as well as the networks of other departments and agencies that process classified information. Regarding defensive cybersecurity policies or actions more broadly, the NSA is a key player on a larger team that includes DHS, FBI, and USCYBERCOM. NSA is an agency with many unique skill sets in offensive cybersecurity policies and actions. NSA can and should advise on U.S. government offensive cybersecurity policies when directed by policymakers, consistent with its authorities.

QUESTION 22: What should be the NSA's role in helping to protect U.S. commercial computer networks?

NSA's mission is fundamentally one of collecting foreign intelligence information and protecting national security systems, though the NSA certainly does contribute great insights into foreign cybersecurity threats that help protect the private sector. Given that cyber attacks of significant consequence on commercial computer networks can cause the loss of life or billions of dollars in damage to an economy, it is paramount that the U.S. public and private sectors work together to create a shared understanding of the threat. If confirmed, I am eager to take part in this collaboration.

QUESTION 23: What cyber threat information (classified or unclassified) should be shared with U.S. private sector entities, particularly critical infrastructure entities, to enable them to protect their networks from possible cyberattacks?

While the responsibility for protecting privately-owned networks lies primarily with the system owner, the U.S. Government has the responsibility to defend national interests more broadly. If confirmed, my goal will be to continue to work with DHS and FBI to try to lean forward and provide unclassified cyber threat information so that it is available for wide public use. When threat information must remain classified, what is shared should depend on factors such as the nature, duration, and severity of the threat, and the ability of the affected entity to receive classified information.

QUESTION 24: It is now well understood that America's election infrastructure is vulnerable to

cyber attacks.

a. If confirmed, how will you address this threat?

I believe this needs to be a whole-of-government solution. DHS and state and local governments are the primary entities leading this effort, and if confirmed I will ensure the NSA and USCYBERCOM continues to support this effort, consistent with their authorities. Our democracy depends on it.

b. What actions should the NSA be taking to protect our election infrastructure for the upcoming November 2018 federal elections?

I completely appreciate the importance of this issue to this Committee and the Nation. NSA will provide support to the government effort, led by DHS, to guard against outside interference in the November 2018 federal elections. If confirmed, I pledge that that effort will have the NSA's full support.

c. How, in your view, should the NSA work with other IC elements to prevent and mitigate threats to our election systems?

I completely appreciate the importance of this issue to this Committee and the Nation. NSA should provide support to the government effort, led by DHS, to guard against outside interference in the November 2018 federal elections. If confirmed, I pledge that that effort will have the NSA's full support, including cooperation with other members of the IC under coordinating direction of a lead agency.

QUESTION 25: In December 2015, the Cybersecurity Act of 2015 was enacted and signed into law, thereby creating a voluntary information sharing process involving both public and private sector entities.

a. In your view, is this process effective?

The process established by the Cybersecurity Act of 2015 was a great first step. I believe the key is bi-directional information sharing. If confirmed, I will seek to better understand the frequency with which this is occurring.

b. What recommendations do you have for this process going forward?

If confirmed, I will be better able to assess and provide more informed recommendations on this issue.

NSA Capabilities

QUESTION 26: What is your assessment of the quality of current NSA intelligence analysis? If confirmed, what additional steps would you take to improve intelligence analysis, and what benchmarks will you use to judge the success of future NSA analytic efforts?

From my previous experience at the NSA, I can say that I expect to find that the NSA presently has a robust intelligence analysis program. NSA analysts are trained in the tradecraft of analysis, and they do it well. To ensure that this program continues to improve, I believe that continuous career growth is essential for current employees. The success of future NSA analytic efforts would be judged by the feedback of our customers, principally the Nation's policymakers and military commanders, on the quality and usefulness of our foreign intelligence reporting.

QUESTION 27: What is your view of strategic analysis and its place within the NSA? Please include your views about what constitutes such analysis, what steps should be taken to ensure adequate strategic coverage of important issues, and what finished intelligence products NSA should produce.

Strategic analysis is analysis that is generally more forward looking or that tries to take several pieces of intelligence analysis and examine them for themes, patterns, or concepts in order to address larger issues. Based on past experience, I believe the NSA must be competent in this discipline so that it can assess the value of its reporting at informing strategic analysis, but the overall role of strategic analytic reporting itself falls to all-source intelligence agencies. In this way, strategic analysis is occurring every day at the NSA but not in the formal sense that it does at all-source reporting agencies.

QUESTION 28: What are your views concerning the quality of intelligence collection conducted by the NSA, and what is your assessment of the steps that have been taken to date to improve that collection?

From my previous experience at the NSA, I can say that I expect to find that the quality is of very high value. I believe the NSA has historically succeeded in response to changes in missions and technology. If confirmed, I will be better able to assess and provide more informed recommendations on this issue.

QUESTION 29: If confirmed, what additional steps would you pursue to improve intelligence collection and what benchmarks will you use to judge the success of future collection efforts by the NSA?

First, I would make a comprehensive assessment in order to better understand current challenges and performance and determine what actions are necessary to improve collection. The success of future collection efforts ultimately must be judged by the feedback of our customers,

principally the Nation's policy makers and military commanders, on the quality and usefulness of our foreign intelligence reporting that results from our collection efforts. NSA does not collect foreign intelligence for its own purposes but in response to its customers' intelligence requirements, so ultimately, any benchmark must take into account their views.

QUESTION 30: What are your views on the role of foundational research to NSA's mission?

From my previous experience at the NSA, I can say that I expect to find foundational research remains a core component to its success. I am aware that the NSA has a robust in-house research organization that has conducted pioneering research since the Agency's creation. If confirmed, I will be better able to assess and provide more informed recommendations on this issue.

NSA Personnel

QUESTION 31: The Committee's most recent Intelligence Authorization bill, as well as the *Intelligence Authorization Act for Fiscal Year 2017* (P.L. 115-31), included provisions supporting IC employment of those with science, technology, engineering, and mathematics (STEM) backgrounds and expertise. If confirmed, how would you undertake outreach, recruitment, and retention of employment candidates with STEM experience?

Recruiting, training, retaining, and empowering the best and brightest our Nation has to offer is mission critical for the NSA. If confirmed, I will ensure that the NSA has a culture where employees can thrive and feel proud of their mission. I understand that this committee has led an effort in the 2018 Intelligence Authorization Act to ensure certain STEM employees in mission critical roles can receive more compensation, and I am supportive of that effort. In my experience, people who work at the NSA understand there is a mission side to their job and don't expect salary comparable to the private sector, but it's important that the Agency have some flexibility with compensation to remain as financially attractive as possible.

QUESTION 32: What is your view of the principles that should guide the NSA in its use of contractors, rather than full-time government employees, to fulfill intelligence-related functions?

a. Are there functions within the NSA that are particularly suited for the use of contractors?

The Federal Government, including the Department of Defense, and the Intelligence Community has long history of successfully using contractors. I will be better able to assess specific examples relevant to this question if confirmed, but I believe there are certainly functions for which the NSA can use contractors to achieve a positive outcome with savings to the taxpayer.

b. Are there some functions that should never be conducted by contractors, or for which use of contractors should be discouraged or require specific DIRNSA approvals?

Contractors should not perform work roles and functions that are inherently governmental in nature. Presently, I lack in-depth insight into specific work roles or functions; if confirmed, I would seek to understand this through discussions with appropriate NSA personnel.

c. What consideration should the NSA give to the cost of contractors versus government employees?

It is important to have the right workforce mix between civilian and contractor employees. If confirmed, I will take into account the costs associated with either role in order to ensure the NSA has achieved the right mix.

d. What does the NSA need in order to achieve an appropriate balance between government civilians, military personnel, and contractors?

Foremost, is careful understanding of the Agency's functional requirements. First, understanding which functions are inherently governmental and not appropriate for contract personnel. Second, determining what balance of personnel best fulfills functional requirements in each area and the cost tradeoffs associated with it. If confirmed, I intend to explore this area more.

QUESTION 33: If confirmed, what will you do to ensure that there are equal professional opportunities for all members of the NSA workforce?

If confirmed, I will ensure equal professional opportunities for all the NSA workforce through several important efforts. First, I will demonstrate through my words and deeds that diversity is a key component of the Agency's success. Second, I will support the continued work by the Agency to ensure facilities are available to all people, with or without disabilities. Finally, I will look to measure the Agency's progress with diversity, ensuring our workforce and leadership are reflective of both the people who work at the NSA and our Nation.

QUESTION 34: What is your assessment of the personnel accountability system in place at the NSA?

It is my understanding that the NSA has robust measures to hold personnel accountable for their actions. There is an independent Inspector General, confirmed with the advice and consent of the Senate, who identifies and investigates wrongdoing. There is a strong Equal Employment Opportunity program, and there are investigations, both routine and special, of security issues. My impressions may be dated, but as I saw during my past assignments at NSA, the Agency uses these programs to hold personnel accountable as appropriate.

QUESTION 35: What actions, if any, should be considered to ensure that the IC has a fair process for handling personnel accountability, including serious misconduct allegations?

Speaking just from my previous experience at NSA, I believe equitable processes must be in place that ensure for appropriate due process, and the independence of the Inspector General must be sacrosanct. This is a very important area for further assessment, if I am confirmed.

Security Clearance Reform

QUESTION 36: What are your views on the security clearance process?

I am aware the Director of National Intelligence has ongoing efforts to examine and reform the security clearance process. I support these initiatives as I believe the current process is challenged by large backlogs of unfinished background investigations, lacks the technology that might enhance broader data points, and takes too long to complete a background investigation and final clearance to empower a trusted workforce.

QUESTION 37: If confirmed, what changes, if any, would you seek to make to this process?

I do intend to fully support any pilot that provides the opportunity to improve the background investigation and security clearance process, leading to both greater effectiveness and efficiency to recruit and hire an elite, trusted workforce. If confirmed, I will evaluate the proposals presented and make an assessment of the changes that might be necessary.

Management of the National Security Agency

QUESTION 38: In what ways can DIRNSA achieve sufficient independence and distance from political considerations to serve the nation with objective and dispassionate intelligence collection and analysis?

If confirmed, I pledge to this Committee that I will follow in the footsteps of my predecessors to ensure NSA continues its long tradition of providing professional, non-partisan intelligence to any administration. Specifically, I will maintain and continue to encourage an environment where analysts can feel comfortable creating accurate intelligence assessments, without regard for the policy implications of any particular assessment.

a. If confirmed, how will you ensure this independence is maintained?

I have spent 31 years in the United States Army, over half of which have involved providing intelligence to policy makers or military leaders. If confirmed, I will look to ensure the Agency's independent approach to analysis is maintained by dedicating the organization to effective collection, objective analysis, and dispassionate reporting of conclusions as part of the larger intelligence community. I will make it clear to leaders throughout the organization that the NSA's first duty is to the Nation.

b. What is your view of DIRNSA's responsibility to inform senior Administration policy officials or their spokespersons when the available intelligence either does not support or contradicts public statements they may have made?

The DIRNSA, like all leaders of the intelligence community, has a responsibility to communicate clearly the analysis and conclusions of their organization. If there is a disconnect with public statements, the DIRNSA then has a responsibility to re-communicate those conclusions to Administration officials.

QUESTION 39: How would you resolve a situation in which the assessments of your analysts are at odds with the policy aspirations of the administration?

I do not believe there is anything to resolve in such a situation. Clearly, the responsibility of intelligence analysts is to make objective assessments and report their best judgment and conclusions independent of such considerations. If confirmed, I would communicate the Agency's conclusions objectively without regard to such conflicts.

QUESTION 40: What are your views of the current NSA culture and workforce?

a. What are your goals for NSA's culture and workforce?

If confirmed, my goals for NSA's culture and workforce center on emphasizing the uniqueness and importance of the NSA's mission with each person who works for the Agency. The phrases that greet each employee as they enter into the Agency, like "Defend the Nation" and "Secure the Future" capture the criticality of what the NSA does each day. I intend to make this a focal point of what the Agency does, in concert with upholding full compliance with our laws and the protection of Americans' Constitutional rights.

b. If confirmed, what are the steps you plan to take to achieve these goals?

I would look to achieve these goals through strong and engaging interaction with the workforce where I can provide my message; a continual dialogue with leaders within the Agency; a broad strategic messaging campaign that touches all parts of the Agency; and ways to leverage feedback as to the effectiveness of this message and its impact on the workforce.

c. How will you strengthen the relationship between the civilian and military members of the NSA workforce?

I believe a close working relationship between the Director and Deputy Director sets the tone for effective relationships between the civilian and military members of the NSA workforce. If confirmed, I would also look to empower both civilian and military leaders in key leadership

positions. Finally, I would seek training and education venues that explain both the similarities and differences of the civilian and military workforce components to ensure greater understanding of the important roles each plays in accomplishing the Agency's mission.

Transparency

QUESTION 41: Do you believe that intelligence agencies need some level of transparency to ensure long-term public support for their activities?

Yes. Public trust is foundational to the Intelligence Community's ability to conduct its activities, and transparency to Congress and to the public is a critical part of earning and maintaining that trust.

QUESTION 42: If confirmed, what would be your approach to transparency?

Given that many details about the NSA's activities must remain classified, it is important that we have the public's trust in what we do. Transparency plays a vital role in gaining and maintaining that trust.

My approach to transparency involves multifaceted objectives. First, the NSA must be open and honest with its overseers, both in Congress and across the Executive and Judicial branches. Because of the inherent confidentiality in much of the Agency's work, NSA's overseers act as a surrogate, ensuring on the public's behalf that the Agency carries out its activities in a manner consistent with the rule of law.

Second, to the extent possible, the NSA must make available to the public information about its activities in a manner that enhances public understanding without jeopardizing sensitive sources and methods. Sharing information with the public is critical to facilitating responsible discussions about the manner in which the Agency executes its mission and it engenders public trust in the NSA.

Disclosures of Classified Information

QUESTION 43: In your view, does the NSA take appropriate precautions to protect classified information and prevent, deter, investigate, and punish unauthorized disclosures of classified information?

I believe that many appropriate precautions are in place; but that recent events demonstrate a need to re-validate and improve in this area. Presently, I am unable to make a fully informed judgement of this question; therefore, if confirmed, I intend to evaluate ongoing efforts to better secure the network and secure the environment before providing my full assessment.

QUESTION 44: If confirmed, how will you ensure that appropriate and necessary precautions to protect classified information are maintained and improved, if necessary?

If confirmed, I will better be able to assess what improvements, if any, are necessary. More broadly, protecting classified information is vital for the NSA to execute its mission successfully. Ensuring continuation and enhancement of the effective improvements made over the last several years will be a primary focus for me.

QUESTION 45: If confirmed, how would you manage, and what priority would you give, to addressing the following issues:

a. The vulnerability of NSA information systems to harm or espionage by trusted insiders;

b. The vulnerability of NSA information systems to outside penetration;

c. The readiness of NSA to maintain continuity of operations;

d. The ability of NSA to adopt advanced information technology efficiently and effectively; and

e. The NSA's recruitment and retention of skilled STEM and information technology professionals, including contractor personnel.

If confirmed, my priorities for the NSA will be to recruit and retain top talent, improve signals intelligence (SIGINT) collection against critical adversaries, and ensure the security of NSA's network and enterprise. Each of these above issues falls within these top priorities. I see each of these issues as significant components of the proposed priorities.

QUESTION 46: How do you think that individuals who mishandle, intentionally or unintentionally, classified information should be dealt with? Would you draw distinctions based on intent?

Mishandling classified information is an incredibly serious matter. Criminal penalties and workplace discipline, including termination and revocation of security clearances, are all options that should be considered based on the facts of the situation. Intent is certainly relevant under the law and certain internal procedures, but the specifics of when and how it matters are difficult to discuss without the facts of a particular case.

QUESTIONS FOR THE RECORD

From Senator Feinstein

Security/Insider Threats

I am greatly concerned about the security at NSA. Some of the worst threats we have had over the past decade to national security of the United States have come from within. In particular, two NSA contractors stand out to me – Edward Snowden and Hal Martin – as particularly egregious.

1. **What concrete steps will you take to address the insider threat issue at NSA?**

If confirmed, I will take several concrete steps, building on the extensive work NSA has already completed and briefed in detail to the Committee. I will look at potential necessary technological changes. I intend to review security clearance procedures, and I will seek input on whether additional authorities are required. I find leaks of classified information reprehensible, I consider their damage to national security grave and unacceptable, and I will vigorously hold all personnel accountable to stop leaks and compromises. Additionally, I will submit crimes reports to the Department of Justice when I believe an unauthorized disclosure of classified information, or other potential Federal crime, has occurred.

2. **What steps will you take to better secure your networks?**

I will provide a detailed answer via classified channels.

Industry Help in Insider Threats

Last week during a hearing on Security Clearance Reform, the Committee heard from Industry leaders that they continue to need better sharing of information from the Federal government.

Industry leaders identified a situation where the government will tell a contractor, "This person is no longer suitable. Take them off the contract." But the government won't tell them why. They won't tell them what behavior has occurred or why they're no longer suitable for the contract, leaving the industry to figure out what happened, if they have the time or resources to do so.

3. **What specific steps will you take to ensure these contractors with problems don't just come back on under a different contract with a different company?**

I believe that with greater sharing of information between the Federal government and the contractor base, we will be able to better ensure that contractors with problems do not just come back under a different contract with a different company. As noted below, NSA may need new authority to facilitate this sharing.

4. **Some potential solutions might require legislation. What efforts do you believe would be helpful?**

I am told that the Federal government is not allowed to share information concerning the suitability of civilian employees with contractors, and that contractors are barred from sharing similar information with the government. This inability to share is a barrier to best security practices. This is where, if confirmed, I may need the help of the Committee in the form of new authority.

Use of Contractors

I continue to be concerned about the general use of contractors in the Intelligence Community. Previously, I worked with Director Panetta and others to reduce the percentage of contractors being utilized, and I've been pleased to see the continued decrease of contractors as a percent of the overall workforce.

Government contractors are supposed to be used only if they are performing tasks that are NOT an inherent governmental function. Intelligence collection clearly is an inherently governmental function. This should not be done by outside individuals.

It is my view that Intelligence Community (IC) functions are largely inherently governmental in nature and that the IC's reliance on contractors should be further minimized.

5. **Do you agree that intelligence work is clearly an "inherently governmental function"?**

I wholeheartedly agree that contractors may not perform any inherently governmental function, and the direction and control of intelligence operations is an inherently governmental function. However, intelligence work includes many activities, some of which are in support of NSA's intelligence mission but do not amount to inherently governmental functions. I believe we should regularly look at the balance between government and contractors as part of NSA's overall workforce.

6. **What is the right balance in your opinion between contractors and government employees?**

NSA must always have qualified and experienced government personnel in key roles, and government personnel should always lead mission functions. NSA must also ensure that it has sufficient government personnel to maintain control over functions that are core to the Agency's mission and operations. If confirmed, I will seek the specifics of the current government employee-contractor mix, and attempt to achieve an ideal balance.

7. **Will you commit to assuring contractors are not permitted to perform inherently governmental functions?**

Absolutely.

From Senator Collins

Lieutenant General Nakasone, in your responses to the Committee's prehearing questions regarding threats to America's election infrastructure, you stated that it would take a "whole-of-government solution," with NSA supporting the effort.

1. Please describe that effort in detail; how do you foresee the NSA engaging with Congress, the Department of Homeland Security, and state government officials to address these threats, particularly with regard to the upcoming the November 2018 federal elections? Will you ask Congress for new authorities if you determine they are needed to adequately protect America's election infrastructure?

Cyber defense requires a whole-of-government effort, with DHS as the Federal government lead for the critical infrastructure and key resources, including U.S. election systems. NSA plays a significant role in helping protect election infrastructure by making available to DHS, and other agencies, the cybersecurity information NSA acquires in the course of its signals intelligence (SIGINT) and cybersecurity missions. Consistent with its mission, DHS can use this information, as well as information obtained from other sources, to assist state governments in their efforts to address threats to election infrastructure.

If confirmed, I will look to ensure that NSA is making full use of appropriate authorities and is thoroughly and effectively integrated with its partners to make available to DHS cyber threat information critical to protecting our elections. I will keep this Committee informed of those threats and of NSA's efforts to assist these entities. As with all of NSA's activities, if I learn that NSA has insufficient statutory authority to conduct its missions I will share my findings with the Committee.

Protection of America's critical infrastructure necessitates rapid and fulsome sharing of cyber threat indicators between the public and private sector actors.

2. If confirmed, what steps would you take to ensure that the NSA is doing everything possible to facilitate the efficient and effective sharing of cyber threat indicators, both within and external to the Intelligence Community, where U.S. critical infrastructure is at risk?

The passage of the Cyber Information Sharing Act of 2015 was an important first step that promotes sharing of cyber threat indicators both within the government and bi-directionally with the private sector. With the vast majority of the critical infrastructure owned or operated by the private sector, increasing this exchange of threat information at "cyber speed" will make these sharing efforts even more impactful. If I am confirmed, I will evaluate the methods and processes with which NSA is sharing cyber threat indicators with DOD, the IC, and DHS's National Cybersecurity and Communications Integration Center whose mission is to create shared situational awareness of malicious cyber activity, vulnerabilities, incidents, and mitigations among the public and private sector.

In your responses to advance hearing questions from the Senate Armed Services Committee, you indicated that recruiting and retaining top talent will be among your priorities as Director of the National Security Agency. Leaders from across the Intelligence Community have described the commercial sector as an increasingly acute source of competition for the technical expertise and aptitude upon which NSA's success is predicated.

3. What policies do you intend to propose to make NSA more attractive as an employer, particularly for technical experts who are in high demand in the private sector?

I believe the solution to this issue is twofold. First and most importantly, I will emphasize the attraction of NSA's unique and important mission to both the current and prospective workforce. For current employees, that means ensuring they can be proud of and feel invested in the work they are doing. For future employees, it means emphasizing the unique opportunities and technologies NSA allows its people to engage and implement in defense of the Nation. Second, I intend to work with this Committee to ensure that previous efforts to increase pay for certain high-attrition STEM roles are reinforced. While in my experience the mission is the most important reason people work for NSA, it is important to narrow the difference in pay between the public and private sector.

NSA is often in direct competition with other government agencies and the private sector for highly qualified cybersecurity professionals. While the private sector can offer higher compensation initiatives, NSA offers entirely unique missions along with a sense of serving the Nation and a greater purpose. There are other critical elements to retaining our STEM workforce. They must have a rewarding career progression and meaningful challenges to stay engaged. I believe in the need to offer specialized, sometimes costly, training opportunities to tie our workforce to retention commitments.

From Senator Wyden

U.S. person queries of EO 12333 collection

> **1.** Under what circumstances, if any, is NSA prohibited from conducting a warrantless U.S. person query of communications collected under EO 12333? If the query is conducted without a warrant, what process is required?

I understand that the Attorney General-approved procedures that govern NSA's collection, processing, and dissemination of SIGINT pursuant to EO 12333 impose significant restrictions on queries that are intended to retrieve the contents of communications to, from, or about US persons. Absent consent of the US person or certain emergency situations, my understanding is that such queries normally must be approved by the Attorney General on a case-by-case basis after a finding of probable cause. Metadata queries follow a different process and procedural requirements. In either event, however, all such queries must be undertaken for a foreign intelligence purpose. Redacted versions of NSA's Attorney General-approved procedures are publicly available.

PPD-28

> **2.** The NSA's January 12, 2015, PPD-28 Section 4 procedures are publicly available. Will you ensure that the NSA continues to post these procedures as well as any modifications, superseding policies and procedures, or significant interpretations?

Yes. According to Section 4(b) of PPD-28, updated or newly issued policies and procedures shall be publicly released to the maximum extent possible, consistent with classification requirements.

Section 702 of FISA

3. Will you undertake a renewed review of the feasibility of estimating the number of communications of Americans or persons inside the United States collected under Section 702 of FISA? Will you commit to working with Congress and outside groups on this issue?

I recognize the importance of this issue. I'm also aware that a significant effort was undertaken recently by NSA to do this. Ultimately, the DNI determined it was not feasible. I understand that NSA and ODNI have shared with this Committee why it is not feasible. If confirmed, I will want to better understand what efforts were explored and why answering this question was determined not feasible to ensure I can better work with Congress on this issue.

Whistleblowers

4. Please describe your commitment to ensuring that NSA personnel and contractor whistleblowers are encouraged, that there will be no reprisals, and that there will be full and timely cooperation with all investigations.

I believe whistleblowing to appropriate entities is an important mechanism for accountability and ultimately strengthens the Agency and the Intelligence Community. If confirmed, I will not tolerate reprisals against those who make protected whistleblower disclosures through appropriate channels and will ensure that the NSA cooperates with all investigations, whether by this committee or the Inspector General.

False statements

5. If you or one of your subordinates were to say something that was factually inaccurate in public, would you correct the public record?

Yes. If I or one of my subordinates makes a materially inaccurate statement in public, I pledge it will be corrected or clarified in public.

Protecting the personal devices and accounts of senior government officials

6. On October 27, 2017, I wrote to Admiral Rogers and then-Acting Secretary of Homeland Security Duke, asking them to take swift action to protect the personal devices and online accounts of senior government officials from targeted cyber-attacks by foreign governments. I have yet to hear back from NSA or DHS about this topic.

a. Do you agree that the personal devices and online accounts of senior U.S. government officials are potentially high-value cyber targets for foreign adversaries?

b. Do you believe that the successful compromise of a senior U.S. government official's personal device or online account can threaten U.S. national security?

c. If confirmed, what, if anything, will you do to protect the personal devices and accounts of senior government officials from cyber-attacks by foreign adversaries?

NSA has a long and successful history securing National Security Systems (NSS). They regularly collaborate with and support technical experts at the Department of Homeland Security (DHS) on cybersecurity issues. If personal devices and accounts, including those of senior government officials, contain work-related information, such devices and accounts would likely be of interest to our foreign adversaries. Successful compromise of such devices and accounts could potentially yield information of intelligence value to our adversaries. If confirmed, I will direct NSA's cybersecurity leadership to continue their cooperation with DHS and determine the authorities and processes under which NSA and DHS could assist senior government officials with personal cybersecurity best practices.

Relations with the FISA Court

7. The declassified version of the April 26, 2017, Memorandum and Opinion and Order of the FISA Court (p. 19) states: "At the October 26, 2016 hearing, the Court ascribed the government's failure to disclose those IG and OCO reviews at the October 4, 2016 hearing to an institutional 'lack of candor' on NSA's part and emphasized that 'this is a very serious Fourth Amendment issue.'"

a. What do you believe should be done to ensure that NSA provides to the Court complete, accurate and timely information?

b. What accountability should apply to NSA personnel who fail to provide this information?

It is paramount that the Foreign Intelligence Surveillance Court have a complete and accurate understanding of the matters over which it has jurisdiction, and that information is made available to the Court in a timely manner. Accordingly, if confirmed, I will ensure there are rigorous processes and procedures in place to meet these commitments. Moreover, I can assure you that I will hold NSA personnel fully accountable for their failure to adhere to these processes and procedures.

Information from foreign partners

8. What limitations do you believe should apply to the receipt, use or dissemination of communications of U.S. persons collected by a foreign partner? How should those limitations address instances in which the foreign partner specifically targeted U.S. persons or instances in which the foreign partner has collected bulk communications known to include those of U.S. persons?

When NSA obtains U.S. person information from a foreign partner, the Agency must handle it in accordance with U.S. law and applicable procedures, including Attorney General-approved procedures governing the conduct of DoD intelligence activities. In addition, no element of the IC may participate in or request any person, including a foreign partner, to undertake activities the element is itself forbidden to undertake.

Impact of foreign governments using commercial, off the shelf malware

> **9.** In his testimony at the March, 2013 Worldwide Threat Assessment of the U.S. Intelligence Community hearing before the Senate Select Committee on Intelligence, then-Director of National Intelligence Clapper described the threat posed by the global market for cyber intrusion software:
>
> In addition, a handful of commercial companies sell computer intrusion kits on the open market. These hardware and software packages can give governments and cybercriminals the capability to steal, manipulate, or delete information on targeted systems. Even more companies develop and sell professional-quality technologies to support cyber operations—often branding these tools as lawful-intercept or defensive security research products. *Foreign governments already use some of these tools to target US systems.* (Emphasis added.)
>
> How significant is the threat posed by foreign governments using lawful-interception software against targets in the U.S., including individuals, businesses, and U.S. government agencies? If confirmed, what will you do to ensure that hostile foreign governments and non-state actors are not able to acquire U.S. made lawful-interception software, or use that technology against U.S. targets?

I certainly recognize the significance of this threat and the dangers it poses. Accordingly, if confirmed, I will work to ensure that NSA provides foreign cyber threat insights such as these to the FBI and other law enforcement agencies, supporting their efforts to prevent the use of software to commit cyber crimes against Americans.

Offensive cyber operations

> **10.** What responsibility does the U.S. government have if a U.S. offensive cyber operation inadvertently affects the computers of U.S. persons or corporations?

It is critically important that our government is doing everything possible to ensure that our effects are limited to the intended targets. In any given case, my response would depend on the particular facts and circumstances of the operation.

From Senator King

1. The Privacy and Civil Liberties Oversight Board (PCLOB) was established by the 9/11 Commission Act of 2007. Its mission is to ensure that the federal government's counterterrorism efforts are balanced with the need to protect privacy and civil liberties. What are your views on the value of the PCLOB?

Oversight of NSA and the entire Intelligence Community (IC) is paramount to ensure, among other things, that intelligence activities are conducted in a manner that protects privacy and civil liberties. The current structure of oversight includes multiple entities across all three branches of government. I believe PCLOB, with its specific mission to oversee the government's adherence to the protection of civil liberties in efforts to prevent terrorism, is a valuable oversight capability. In addition, their July 2014 report on Section 702 of the Foreign Intelligence Surveillance Act illustrates how they can play an important role in promoting transparency, which serves to enhance the public understanding of intelligence activities, while continuing to protect the IC's valuable sources and methods.

2. After CYBERCOM is elevated to unified command status, when do you believe it will be appropriate to end the dual hat relationship between CYBERCOM and NSA? Is this something that should be done immediately? Or, in contrast, should it be done gradually over several years and pursuant to meeting key milestones?

I believe it will be appropriate to end the dual hat when it is clear that it is in the Nation's best interest to do so. That requires that DoD has completed its assessment, has concluded that separation is feasible and desirable, has made the certifications to Congress required by the 2017 NDAA, and has put in place the processes and procedures necessary to ensure that each organization can succeed in its assigned missions while continuing to benefit from close collaboration and support. A decision to terminate the dual-hat status should only be the result of a deliberate process with clear milestones. I project that some measures associated with separation might be immediately implementable while others may need to be accomplished gradually over time. If confirmed, my intent is to look closely at this and provide an assessment to both the Secretary of Defense and the Chairman of the Joint Chiefs of Staff within the first 90 days of my tenure.

3. To what extent does CYBERCOM currently rely on NSA personnel to execute its mission? Once the split occurs, will CYBERCOM need to replicate everything that NSA has been doing? How will this work and how much will this cost?

The National Security Agency (NSA) provides personnel support to USCYBERCOM with 454 authorizations through the Cyber Mission Partnership, and 69 authorizations through the Engagement and Process Coordination program. USCYBERCOM's requirement for NSA personnel support remains enduring with or without the dual-hat arrangement, and these programs have dedicated funding lines across the Future Years Defense Program. USCYBERCOM does not intend to replicate all the capabilities NSA provides, and continued access to NSA's high end capabilities is in the national interest to save the costs of building duplicative infrastructure. USCYBERCOM reimburses NSA for the services provided based on mutually agreed upon rates in Interservice Support Agreements. For Fiscal Year 2017, USCYBERCOM provided $99.3M in reimbursement to NSA for services rendered. Continued support for the Department of Defense's investment in cyberspace capabilities is crucial to maintaining a competitive advantage over determined adversaries in this domain.

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

March 14, 2018

The Honorable Richard Burr, Chair
The Honorable Mark Warner, Ranking Member
U.S. Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Burr and Ranking Member Warner:

In advance of the hearing regarding the nomination of Lieutenant General Paul M. Nakasone to be the Director of the National Security Agency,[1]" we write to you again regarding the need to protect democratic institutions against cyber attack by foreign adversaries.

The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC is a leading advocate for civil liberties and democratic values in the information age, and works closely with a distinguished Advisory Board, with specific expertise in cyber security and voting technology.[3]

After reports emerged about Russian interference with the 2016 election, EPIC launched a new project on Democracy and Cybersecurity.[4] EPIC is currently pursuing four Freedom of Information Act matters to learn more about the Russian interference in the 2016 Presidential election.[5] One of our cases *EPIC v. FBI*, revealed that the FBI failed to follow the "victim notification procedures" with both the DNC and the RNC.

The Russian attacks on democratic institutions are expected to continue.[6] The U.S. Intelligence community has reportedly shared the classified ODNI report with European

---

[1] *Nomination of Lieutenant General Paul M. Nakasone to be the Director of the National Security Agency,* 115th Cong. (2018), S. Select Comm. on Intelligence, https://www.intelligence.senate.gov/hearings/open-hearing-nomination-lieutenant-general-paul-m-nakasone-be-director-national-security (Mar. 15, 2018).
[2] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] *See* EPIC Advisory Board, https://epic.org/epic/advisory_board.html. *See, e.g.,* Douglas Jones and Barbara Simons, Broken Ballots: Will Your Vote Count? (2012); Ron Rivest and Phil Stark, *Still Time for an Election Audit,* USA Today, Nov. 18, 2016.
[4] *See* EPIC, *Democracy and Cybersecurity: Preserving Democratic Institutions*, https://epic.org/democracy/.
[5] *EPIC v. ODNI*, No. 17-163 (D.D.C. filed Jan. 25, 2017); *EPIC v. FBI*, No. 17-121 (D.D.C. filed Jan. 18, 2017); *EPIC Seeks Release of FISA Order for Trump Tower*, EPIC (March 6, 2017), https://epic.org/2017/03/epic-seeks-release-of-fisa-ord.html; *EPIC v. IRS*, No. 17-670 (D.D.C. Aug. 18, 2017).
[6] Declassified ODNI Assessment, *supra* note 7, at 5.

governments to help limit Russian interference with their elections.[7] The public has "the right to know" the extent of Russian interference with democratic elections in the United States and the steps that are being taken to prevent future attacks.[8] The need to understand Russian efforts to influence democratic elections cannot be overstated. Midterm election campaigns in the U.S. are underway and we have not taken adequate protections to ensure that Russia does not again interfere.

Cybersecurity must be a top priority for the United States. The National Security report states the "government must do a better job of protecting data to safeguard information and the privacy of the American people."[9] Strong encryption keeps the information of the American people secure, which by extension makes the nation secure. And perhaps it is a firewall and not a border wall that the United States needs to safeguard its national interests at this moment in time.[10]

EPIC urges the Committee to ask the nominee:

- ***Do you agree with the January 2017 assessment of the Intelligence Community that the Russians interfered with the 2016 Presidential election?***
- ***Do you believe that the United States has taken sufficient steps to prevent Russian meddling in the mid-term elections?***
- ***If confirmed, what actions will you take to protect the United States against future cyber attacks that could destabilize our democratic institutions?***
- ***Do you commit to the American people to be open and transparent about the work of the NSA?***

We ask that this Statement from EPIC be entered in the hearing record. EPIC will keep the Committee apprised of the documents we receive in our FOIA cases. We look forward to working with you on the cybersecurity risks to democratic institutions.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

/s/ Jeramie Scott
Jeramie Scott
EPIC National Security Counsel

---

[7] Martin Matishak, *U.S. shares hacking intel with Europe as Russia shifts focus*, POLITICO Pro (Feb. 6, 2017).
[8] "A people who mean to be their own Governors must arm themselves with the power knowledge gives," James Madison. *See generally* EPIC, *Open Government*, https://epic.org/open_gov/.
[9] *Id.* at 13.
[10] Garry Kasparov (@kasparov63), "If the US is serious about stopping a real danger from abroad, it should build a better firewall, not a bigger border wall." (12:34 PM - 22 Jan 2018), https://twitter.com/Kasparov63/status/955539139121819649.