S. HRG. 119–280

OPEN HEARING: NOMINATION OF LIEUTENANT GENERAL JOSHUA M. RUDD TO BE DIRECTOR OF THE NATIONAL SECURITY AGENCY

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

SECOND SESSION

JANUARY 29, 2026

Printed for the use of the Select Committee on Intelligence

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

U.S. GOVERNMENT PUBLISHING OFFICE

62–707 WASHINGTON : 2026

SELECT COMMITTEE ON INTELLIGENCE

(Established by S. Res. 400, 94th Cong. 2d Sess.)

TOM COTTON, Arkansas, *Chairman*
MARK R. WARNER, Virginia, *Vice Chairman*

JAMES E. RISCH, Idaho
SUSAN M. COLLINS, Maine
JOHN CORNYN, Texas
JERRY MORAN, Kansas
JAMES LANKFORD, Oklahoma
MIKE ROUNDS, South Dakota
TODD YOUNG, Indiana
TED BUDD, North Carolina

RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS S. KING, Jr., Maine
MICHAEL F. BENNET, Colorado
KIRSTEN E. GILLIBRAND, New York
JON OSSOFF, Georgia
MARK KELLY, Arizona

JOHN THUNE, South Dakota, *Ex Officio*
CHARLES E. SCHUMER, New York, *Ex Officio*
ROGER F. WICKER, Mississippi, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*

RYAN TULLY, *Staff Director*
WILLIAM WU, *Minority Staff Director*
KELSEY S. BAILEY, *Chief Clerk*

CONTENTS

JANUARY 29, 2026

OPENING STATEMENTS

WITNESSES

SUPPLEMENTAL MATERIAL

OPEN HEARING: NOMINATION OF LIEUTENANT GENERAL JOSHUA M. RUDD, TO BE DIRECTOR OF THE NATIONAL SECURITY AGENCY

THURSDAY, JANUARY 29, 2026

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

The Committee met, pursuant to notice, at 10:00 a.m., in Room SD–106, in the Dirksen Senate Office Building, Hon. Tom Cotton, Chairman of the Committee, presiding.

Present: Senators Cotton (presiding), Warner, Gillibrand, Rounds, Budd, Young, Kelly, King, Collins, Lankford, Wyden, Ossoff, and Cornyn.

OPENING STATEMENT BY HON. TOM COTTON, A U.S. SENATOR FROM ARKANSAS

Chairman COTTON. I want to begin by welcoming you all to our hearing to consider the nomination of Lieutenant General Joshua M. Rudd to be the director of the National Security Agency. General Rudd has already endured a lengthy confirmation hearing at the Armed Services Committee where he was warmly received. I'm sure he's excited to be back testifying in front of Congress yet again.

I do want to note for the audience that we welcome your attendance to observe the hearing today, but Vice Chairman Warner and I agree that we will not tolerate any disruptions. Anyone who disrupts the hearing will be removed from the hearing room and could face potential further sanctions to include being barred from the Capitol grounds.

As I mentioned, General Rudd has previously testified for his nomination at the Armed Services Committee. Our committee has sequential referral, our goal for this hearing is to consider the nominee's qualifications and give members ample opportunity for thoughtful deliberation. General Rudd has already provided substantive written responses to dozens of questions from this committee.

Today members will be able to ask additional follow-up questions and hear from the nominee directly. Our members are familiar with General Rudd from their visits to PACOM and also from his previous testimony to our committee in closed session where he was also warmly received. I want to take this opportunity to once

again thank General Rudd for his lifetime of service and answering the call once again.

And also, I would like to recognize his wife Ansley, his daughter Hayden, his son-in-law, JT, who are joining us today; welcome. As well as his mom who is watching from South Carolina and his younger daughter, Hollis, who is watching virtually. She was at the Armed Services Committee. I guess she thought better of a repeat performance.

On behalf of this committee, thank you all for your support through this process and for your husband and your dad's decades of military service. General Rudd is a Special Forces officer who currently serves as the deputy commander of the U.S. Indo-Pacific Command. In addition to various special operations and interagency task force assignments, General Rudd has commanded at the platoon, troop, company, squadron, group and combatant command functional component levels.

Among his previous assignments, General Rudd has served as chief of staff for U.S. Indo-Pacific Command, commander of Special Operations Command Pacific, and deputy commanding general for operations for the 25th Infantry Division. If confirmed as director of the National Security Agency, General Rudd will be asked to serve as the head of the NSA and as commander of the U.S. Cyber Command. With this in mind, I look forward to hearing from you about how your wide ranging experience equips and prepares you to fulfill this dual hatted role and assume the enormous responsibility of protecting Americans and our homeland from harm. Again, I want to thank you, General Rudd, for your many years of service to our nation and for your willingness to continue serving our country in this new role.

I now recognize our distinguished vice chairman for his remarks.

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

Vice Chairman WARNER. Well, thank you, Mr. Chairman. And, General Rudd, it's good to see you again and it's great to meet your wife and daughter and son-in-law. Um, again thank you for making time to meet with me the other day. We all know that NSA has been without a Senate-confirmed director for over nine months. Given the sustained pace of cyberattacks against the United States by our adversaries, the complexity of maintaining the world's premier system and the sheer volume of intelligence requirements from combatant commanders, I'm eager to provide the tens of thousands of employees at NSA with steady permanent confirmed leadership.

However, as I told you when we last met, I have a few priorities and I'll need your commitment on them if you want to earn my vote. First and foremost, I remain deeply concerned about the politically motivated firings of career civilian and military leaders across our national security enterprise. That includes the firing of your predecessor, General Tim Haugh.

I worry about the message these firings send that political loyalty is valued over competence. That message risks chilling the ICs' willingness to speak truth to power or even to produce vital intelligence that may conflict with preferred talking points or mes-

saging of the day. So, as we discussed the first time, and I will ask you this in—in my questioning, I just—the IC—if the IC is unwilling to tell policymakers what they need to hear and not just what they want to hear, America is less safe.

So, I will need your commitment that you will always be candid with policymakers, and nothing in your background reflects that you wouldn't be, but that you will always be transparent with Congress and you'll foster a culture at NSA that prizes candor and transparency; including standing up for your workforce if they are unfairly targeted.

Second, as we discussed, I strongly support NSA's traditional SIGINT message, but I also believe there are areas where NSA can and should play a bigger role. One of those areas is technology; that means leveraging existing technologies to make NSA more effective, and it means better targeting our adversaries advances in technologies that weaken American security.

In this endeavor, I hope NSA will lean into strong relationships. Within the U.S. government, for example, we talked about some of the cross-pollination with the Department of Commerce, with the private sector and with allies and partners abroad, which brings me to another priority, strengthening alliances and partnerships.

NSA has deep and long standing SIGINT relationships across the world, especially with our Five Eyes partners, but I suspect that many of our partners are feeling confused and even abandoned. That confusion is driven by tariffs imposed on our close trading partners, by open talk of a military action against a NATO ally and by a defense strategy that walks back our commitments in Europe and the Pacific.

As members of this committee know well, our allies and partners provide critical intelligence that complements our own, and when these relationships are jeopardized, again, America is less safe. Finally, I want to briefly focus on election security. I have often noted, and I know all the members of this committee appreciate it, that it was the credit—to the credit of President Trump during his first term that we built a robust infrastructure to identify adversary attempts to interfere in U.S. elections, to inform the public, and to disrupt and dismantle adversary infrastructure such as troll farms—troll farms.

And as you know, the NSA and prior leadership played extraordinarily important role in all of those activities. So, it is ironic and highly unfortunate that in this term President Trump and his team have literally dismantled that infrastructure they built. While at the same time, senior officials, including the person responsible for leading our nation's intelligence community, appear willing to blur the line between intelligence and domestic political activity.

There are only two explanations for why the Director of National Intelligence decided yesterday to show up at a federal raid tied to the president's obsession with relitigating the 2020 election. First, she believes there is a legitimate foreign intelligence nexus, in which case she has violated her legal obligation to keep this intelligence community and committees fully and completely informed.

Or, she is simply attempting to inject the nonpartisan intelligence community into a domestic political stunt designed to legitimize conspiracy theories that undermine our democracy. Either

scenario represents a serious breach of trust and a dereliction of duty to the solemn office, which she holds. So, I'll be looking to you among others to ensure that we defeat real adversary efforts to mess with our elections and to help ensure that the intelligence community never allows itself to be used to advance political narratives instead of protecting domestic institutions. There are, of course, other issues and I know we had a robust discussion about Section 702, which is going to need reauthorization. I look forward to discussing those—these, issues and many others and working with you as I expect you will be confirmed.

Thank you very much, Mr. Chairman. Look forward to the presentation.

Chairman COTTON. Thank you, Mr. Vice Chairman. General Rudd, before we move to your opening remarks, the committee has a series of standard questions we posed to each nominee that require a simple yes or no answer for the record. Although if the answer is no, there will probably be need for explanation, which is the equivalent of your instructor stomping his foot in an Army study review.

So, here we go. One, do you agree to appear before the committee here and in other venues when invited?

Lt. General RUDD. Yes, Mr. Chairman.

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

Lt. General RUDD. Yes, Mr. Chairman.

Chairman COTTON. Three, 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?

Lt. General RUDD. Yes, Mr. Chairman.

Chairman COTTON. Four, will you ensure that your office and your staff provide such material to the committee when requested?

Lt. General RUDD. Yes, Mr. Chairman.

Chairman COTTON. Five, do you agree to inform and fully brief to the fullest extent possible all members of this Committee of Intelligence activities and covert actions rather than only the chairman and vice chairman?

Lt. General RUDD. Yes, Mr. Chairman.

Chairman COTTON. Thank you, General Rudd. We'll now proceed to your opening statement, after which we'll go to members by seniority at the gavel for five minutes each. General Rudd, the floor is yours.

STATEMENT OF LIEUTENANT GENERAL JOSHUA M. RUDD, NOMINEE TO BE DIRECTOR OF THE NATIONAL SECURITY AGENCY

Lt. General RUDD. Chairman Cotton, Vice Chairman Warner, and distinguished members of the committee, I'm deeply honored and humbled to appear before you today as the nominee for director of National Security Agency, chief Central Security Service and commander U.S. Cyber Command. I want to thank President Trump, Secretary Hegseth, the chairman and the chief of staff of the Army for the nomination and their trust in me to lead this critical national security role.

I would like to acknowledge my family in attendance. First of all, Ansley, my wife, best friend and partner in this journey for the last 35 years. Our daughter Hayden, who works on the Senate Committee on Commerce, Science, and Transportation is also here along with our son-in-law, JT, who is a data scientist and AI engineer.

Our other daughter Hollis, who lives in Texas, couldn't be here, but I know she is watching, along with our extended family in South Carolina. Each of you have—each of you have made profound sacrifices that have been instrumental in my life of service. You have positively impacted our military, their families and civilian communities, and I am eternally grateful for your unwavering support.

My career has also been shaped by the remarkable men and women with whom I've served. I'm particularly indebted to the noncommissioned officer corps whose leadership and professionalism have inspired me for the past three plus decades. And we must always remember and honor our nation's fallen and their families who have made the ultimate sacrifice.

My path in the Army has been unconventional, starting as a logistician before I transferred to Special Forces. This background has given me a unique operational lens. I spent over 25 years leading our nation's special operations missions, integrating high consequence capabilities, which has given me a deep practical understanding on how to use intelligence to drive operational success, while ensuring the protection of our most critical sources and methods.

These leadership roles involve pioneering highly technical solutions through close collaboration with American industry and ensuring these complex multi-domain systems were seamlessly woven into—into operations. My last six and a half years in the Indo-Pacific have made clear that we are witnessing a surge in adversarial activity.

These complex threats are amplified by low cost, widespread proliferation of disruptive technologies including AI, cyber capabilities and autonomous systems, which place advanced capabilities in the hands of a broader range of actors. Today's threats are no longer distant. They are immediate challenges to our critical infrastructure and democracy.

However, through a growing ecosystem of trusted partners in industry and academia, we are developing, experimenting and rapidly improving solutions to address these challenges head on. This relentless pursuit of excellence is central to my personal and professional ethos and it respects—it reflects the spirit of American innovation.

A critical asymmetric advantage that ensures we remain ahead of dynamic adversarial threats. As a leader, consumer, enabler, generator and integrator of NSA and cyber command capabilities, my focus has been on defending the homeland, deterring adversaries and strengthening partnerships by delivering credible technologically advanced capabilities in all domains.

If confirmed, I am prepared to lead these organizations as an integrated and essential team dedicated to increasing the speed and agility of our support for the nation's toughest challenges while cul-

tivating and retaining a uniquely qualified workforce. Central to this will be the delivery of accurate and timely intelligence, advice and options always conducted with frequent transparent communication with Congress and absolute fidelity to our Constitution.

With this committee's support, my focus will be to lead the NSA in its vital foreign intelligence mission driven by the pursuit of innovation with a commitment to unbiased objective analysis. Thank you for the privilege of appearing before you today. If confirmed, I look forward to working with you closely and I look forward to your questions.

[The written statement of the witness follows:]

LTG Joshua Rudd, Opening Statement for SSCI, January 29, 2026

Chairman Cotton, Vice Chairman Warner, and distinguished members of the committee, I am deeply honored and humbled to appear before you today as the nominee for Director of the National Security Agency, Chief of the Central Security Service, and Commander of U.S. Cyber Command. I want to thank President Trump, Secretary Hegseth, the Chairman, and the Chief of Staff of the Army for the nomination and their trust in me to lead this critical national security role.

First, I would like to acknowledge my family. My mother, who is observing us today from South Carolina; my wife, Ansley; our two daughters and our son-in-law. Each of you have made profound, often understated, sacrifices that have been instrumental to my life of service, and have positively impacted our military, their families, and civilian communities. Your presence here today is a testament to your unwavering support, for which I am eternally grateful.

My career has been shaped by the remarkable men and women with whom I have served. I am particularly indebted to our Non-Commissioned Officers Corps, whose leadership and professionalism have inspired me for the past three plus decades. Finally, we must always remember and honor our nation's fallen and their families, who have made the ultimate sacrifice.

My path in the Army has been unconventional, starting as a logistician before I transferred to Special Forces. This background has given me a unique operational lens. I spent over 25 years leading our nation's special operations missions; integrating high-consequence capabilities, which has given me a deep, practical understanding in how to use intelligence to drive operational success, while ensuring the protection of our most critical sources and methods. These leadership roles involved pioneering highly technical, and increasingly digital, solutions through close collaboration with American industry, and ensuring these complex, multi-domain systems were seamlessly woven into operations.

My last six and a half years in the Indo-Pacific have made clear that we are witnessing a surge in adversarial activity. These complex threats are amplified by the low-cost, widespread proliferation of disruptive technologies, including artificial intelligence (AI), cyber capabilities, and autonomous systems, which place advanced capabilities into the hands of a broader range of actors.

Today's threats are no longer distant. They are immediate challenges to our critical infrastructure and democracy. However, through a growing ecosystem of trusted partners in industry and academia, we are developing, experimenting, and rapidly improving solutions to address these challenges head-on, through agile cycles of improvement against real-world application. This relentless pursuit of excellence is central to my personal and professional ethos and reflects the spirit of American innovation, a critical asymmetric advantage that ensures we remain ahead of dynamic adversarial threats.

As a leader, consumer, enabler, generator, and integrator of NSA and Cyber Command's capabilities, my focus has been on defending the homeland, deterring adversaries, and strengthening partnerships by delivering credible, technologically advanced capabilities in all domains.

If confirmed, I am prepared to lead these organizations as an integrated and essential team, dedicated to increasing the speed and agility of our support for the nation's toughest challenges and cultivating and retaining a uniquely qualified workforce. Central to this will be the delivery of accurate and timely intelligence, advice, and options, always conducted with frequent, transparent communication with Congress and absolute fidelity to our Constitution. With this Committee's support, my focus will be to lead the NSA in its vital foreign intelligence mission, driven by the pursuit of innovation and an unwavering commitment to unbiased, objective analysis.

It is a privilege to appear before you today and if confirmed, I look forward to working with you closely. Thank you and I look forward to answering your questions.

Chairman COTTON. General, you have an extensive career as a special forces operator. You've deployed numerous times on combat operations in the Middle East and the Pacific. During that career, we've seen cyber play an increasing role in special forces operations. Could you give us a flavor of how you've used or supported cyber operations throughout your career and what lessons you've learned from that?

Lt. General RUDD. Yes, Mr. Chairman, the—the vast amount of joint combined and interagency leadership roles that I've had the privilege to fulfill throughout my career, especially in combat operations, has generated an experience that is rich and replete with examples where I've worked closely with the interagency.

Again, the—the most recent example that I can share on that one was the, you know, committee briefing that we had previously with one of our agency partners. Um, so, a rich experience of—of working collaboratively across interagency. But more specifically to NSA and Cyber Command throughout—through out my career, the—the foreign intelligence capability and the mission set of the NSA has informed and certainly enhanced and enabled the mission outcomes in a variety of mission sets.

Equally paired is experience with Cyber Command and cyber capabilities. They work hand-in-hand, they work best when they're integrated across the joint force and in all domains. And increasingly when we think about and talk about deterrence, there's opportunity to couple what DOD is doing with the whole of government.

Chairman COTTON. Thank you. As I mentioned at the outset and you alluded to, this is technically two jobs, NSA director and the commander at Cyber Command. How have you thought about balancing the roles of those two jobs and ensuring that both missions are executed effectively?

Lt. General RUDD. So, Mr. Chairman, I think I would draw upon my experience right now at USINDOPACOM as an opportunity to learn and highlight the responsibility of INDOPACOM, not only geographically is vast, but its pans the entirety of the joint force. It has over 300,000 assigned forces. So, as—to your point, two—two giant organizations that I would be responsible, if confirmed for this, I think the scale in the size of it are manageable.

What I would hope to do, if confirmed, is ensure that the unique capabilities, the unique authorities that both of these organizations bring to bear are fully integrated both within support and interdependence of each other's missions, but then in support of the warfighter and providing the best option to our decision makers.

Chairman COTTON. CYBERCOM is significantly smaller than NSA. Have you developed any thoughts yet on how that organization might need to grow or change to ensure the missions are balanced?

Lt. General RUDD. Well, Mr. Chairman, one of my priorities, if confirmed for this, would be scale across both organizations, not only in the workforce, but also in the capabilities, the technologies and how we enhance that. But my understanding is there is a deliberate approach in, in, in effect right now under CYBERCOM 2.0 to man, train and equip the cyber force.

Certainly, if confirmed, I would like to understand how that's being implemented, are there ways to accelerate it and then provide best advice on how to do that.

Chairman COTTON. As the vice chairman noted in his opening remarks, FISA Title VII specifically Section 702, expires in less than three months unless Congress reauthorizes it. Section 702 explicitly—explicitly applies to foreign nationals on foreign territory. Can you talk to us about how critical Section 702 is for the NSA's mission and how detrimental it would be if the authority expired?

Lt. General RUDD. Senator, or Mr. Chairman, from an operational perspective as you highlight, that foreign intelligence mission focuses on non-U.S. persons outside the U.S. As—you know, throughout my career and my firsthand experience as a consumer of that intelligence and enabler to those capabilities, it's indispensable.

I know it's been critical to mission outcomes. Its force protection of our men and women in harm's way, and I know it saved lives, uh, here in the homeland.

Chairman COTTON. Thank you. Vice Chairman.

Vice Chairman WARNER. Thank you, Mr. Chairman, and, again, general, enjoyed our conversation and I'm going to ask you a couple of questions, which, uh, you can simply answer, yes or no as well. Uh, I have great faith that you will answer, yes, but I want to make sure we get these on the record. First, do I have your commitment that if you're confirmed that you will stand up for your workforce if they are unfairly targeted?

Lt. General RUDD. Mr. Vice Chairman, you do.

Vice Chairman WARNER. Thank you. Do you have—do I have your commitment, and this is one of the things I'm extraordinarily concerned about. You know, the ICs got to speak truth to power and so, do I have your commitment you will always be candid with policymakers, even if you have to tell them something they don't want to hear?

Lt. General RUDD. Mr. Vice Chairman, I will, and you do have my commitment.

Vice Chairman WARNER. I think your record reflects that. One of the things, and again I touched on this in my opening statement, where the Director of National Intelligence is suddenly appearing, uh, at a FBI raid around elections from frankly 2020, which I have no idea what she was doing there. But I am concerned that we've seen much of the election security infrastructure that was put in place extraordinarily well by the first Trump administration, where, again, the NSA played a critical role, be dismantled and there's no less threat from foreign adversaries about trying to mess with our elections.

So, do I have your commitment that if confirmed that the NSA will continue to prioritize information sharing on threats to U.S. elections, on foreign threats to U.S. elections?

Lt. General RUDD. Mr. Vice Chairman, you do. The electoral process is fundamental to our values, our way of life. And throughout my entire career, I've been committed to upholding those and protecting those. I think anything that poses a threat to the electoral process needs to be taken seriously.

And if confirmed, Mr. Vice Chairman, I commit to working with the executive and the legislative on this.

Vice Chairman WARNER. Thank you. Because, again, the NSA and particularly in the 2018 through 2020 cycle played a very important role. This is something we've not talked about, but we all know AI has enormous potential, um, and both DOD and the intelligence community is looking to take advantage of those AI capabilities. But we also know that there's a number of AI tools that still have a tendency to hallucinate and, um, with that tendency, sometimes it poses major security risks.

I've been concerned that Secretary of Defense Hegseth has um—starting to unleash AI both across classified and unclassified networks, including models such as xAI's Grok model, which has got, again, more of a history of hallucination than most. If confirmed, will you ensure that appropriate policies are in place to stand, safeguard, DOD and NSA's critical mission and that while we use these AI tools that there are appropriate safeguards?

Lt. General RUDD. Mr. Vice Chairman, this is a critical area of competition and I know INDOPACOM is relying heavily on the adoption of AI, and I suspect, and expect, that CYBERCOM and NSA are as well. In fact, I know they are. My understanding and really the approach that we've taken with the adoption of these technologies is while they are absolutely imperative to advancing our skill set as joint warfighters enabling us decision superiority.

We will never abdicate our responsibility to maintain those guardrails. The guardrail is the human on the loop or in the loop in terms of what those technologies are providing, what they're producing and then how we apply them. So, you have my commitment. Thank you Mr. Vice Chairman.

Vice Chairman WARNER. Thank you. I look forward to working with you on that. Finally, and I know, and this was in, over at SASC. I think in your testimony, you noted, North Korea's heavy reliance on cryptocurrency. I'm in the midst of, looking around the table, I don't think any of my colleagues are as deeply involved in trying to make sure we've got some rules of the road around market structure for crypto.

I think it's going to be an incredibly important part of our financial system going forward, but boy, it is complicated. So, do you believe that the federal government needs to do more across the interagency to track, disrupt and abate foreign malign actors access to these digital ecosystems?

Lt. General RUDD. Mr. Vice Chairman, that's something that I would have to take a closer look at. Certainly, we're looking at it from an INDOPACOM lens on what it means for national security and implications. But, Mr. Vice Chairman, if confirmed, I commit to looking at——

Vice Chairman WARNER. My time's up but I just want to make the comment that you—crypto has great possibilities, it's not going away. But boy, oh boy, there are some national security implications around this that we have to get, right.

So, thank you.

Thank you, Mr. Chairman.

Chairman COTTON. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman. General, I want to follow up on a discussion that we had in our meeting and it relates to some degree to questions that have already been raised. I have been greatly concerned about cybersecurity issues affecting all branches of government, the private sector and our critical infrastructure.

Ransomware attacks and Salt Typhoon intrusions continue at an alarming rate. However, when it comes to the federal government's defensive and offensive capabilities, we seem to be stove piped. There's a cyber czar, FBI's involved, CISA, your predecessor, have all used terms like team effort, collaboration, coordination, and yet there appears to be no lead.

And yet we see these ongoing attacks that get ever worse. In fact, just last month, another Salt Typhoon intrusion was detected against staff of the House of Representatives. So, we need to stop Salt Typhoon intrusions. We need to secure our critical Infrastructure from being taken over by hostile actors.

We've seen in the state of Maine hospital data being hacked with some of the most sensitive data possible. What can we do to detect, cease and get ahead of these cyber intrusions?

Lt. General RUDD. Senator, again, I appreciate the opportunity to meet and thanks for the time. On this particular topic, first and foremost, it's aggressive vigilance. We have to understand what the threats are, where they emanate from and then what are the options of capabilities that can be applied. And then to your point about the various entities across the government that have responsibility for this, my experience says continuous collaboration coordination, unity of effort is what makes us most effective in that, and if confirmed for this role, I would pledge to be a part of that.

Senator COLLINS. Do you see yourself as the lead in trying to combat this ever increasing threat?

Lt. General RUDD. Well, Senator, I see us as a lead from the department and from the military aspect, certainly on the cyber capability piece of this question. Um, I don't know that we've been designated the lead for this effort.

Senator COLLINS. I think that's part of the problem, that we do need a designated lead. Let me switch to another issue. We understand that the Department of Defense has prioritized the effective adoption of artificial intelligence to secure American military AI dominance. My understanding is that this is meant to help drive efficiencies and improve decision making.

The adoption of these technologies, however, is not without risk. It has the potential to introduce significant cyber risk if the AI systems themselves are not properly protected and managed. As the incoming director of NSA and Cyber Command, how will you bridge that gap between the adoption of AI and AI security?

Lt. General RUDD. Well, Senator, I think that's a critically important topic and with any new technology, there's always risk. But what I see in this particular technology is an imperative that we adopt it, apply it, understand it. And to your point, how do you secure it? I know there's efforts going on right now within NSA around AI security that extends through collaboration and Intel driven recommendations to commercial partners.

And certainly we have to make sure that we protect that.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman COTTON. Senator King.

Senator KING. Thank you, Mr. Chairman. General, we have talked in the past about this question of cyber and one of the huge gaps in our cyber policy in this country is the lack of any cyber deterrent. Our adversaries pay no price for their attacks; whether it goes back to the Sony hack or the recent, Volt and Salt Typhoon.

Do you believe that it would be important for us to establish a deterrent strategy that our adversaries would be aware of and would color their decision making as to whether or not to launch an attack, a cyberattack, against this country?

Lt. General RUDD. Senator, thanks for the opportunity to meet, and I appreciate the opportunity to revisit this topic. The short answer is yes, I do.

Senator KING. I appreciate that and I think that's very important and I hope you'll work with NSA and CYBERCOM to develop that capacity because otherwise we can never patch our way out of this problem. The adversaries are going to continue to evolve. And at some point, we have to make them have second thoughts about whether to attack this country in cyberspace.

Second question, I just want to reiterate your conversation with the—with the vice chairman. It's so important that our intelligence community provide candid, clear, unvarnished, nonpolitical advice to policymakers, uh, because otherwise, we have—we can have real catastrophes involving our national security.

So, I just want to reiterate that you answered the question, yes. You're committed to that. It's somewhat easy to answer that question here, it's going to be a little harder in practice if you're sitting in the Oval Office or in some other setting that is inherently intimidating. Uh, but I want you to reiterate your commitment.

Straight talk, straight advice and the facts to the policymaker, is that correct?

Lt. General RUDD. Senator, I am committed to that, as I have been throughout the entirety of my career. I pride myself on a leader who has always been candid and given best advice even if it wasn't popular.

Senator KING. Thank you. Final area. In your work in INDOPACOM, I know you came to realize the value of the allies that we have in the Pacific. In my work on this committee and the Armed Services Committee, I've come to realize our asymmetric advantage in the world is allies. China has customers, we have allies.

Russia doesn't have much in the way of customers or allies. But it's so important to maintain those relationships; particularly in the intelligence community. Talk to me a little bit about the Five Eyes and how important it is to maintain that intelligence sharing enterprise and particularly to—to be sure that there's a trusting relationship so that we will have the maximum advantage of the—of the ability of our—of our allies to work with us in order to protect the national security of this country.

Lt. General RUDD. Senator, I've had the incredible fortune throughout my career to serve alongside with and through allies and partners. I think our strategic documents identify clearly the importance of that and the emphasis that—that we put on that. The Five Eyes in particular some of my closest colleagues in profes-

sional relationships are within that community and certainly rely upon them.

As—as it relates to INDOPACOM, it's a—it's a daily effort. We have embedded liaison officers from throughout our allies and partners within the region and it's a consistent engagement. We operate together, we exercise together, we train together and that's part of our strategic approach to delivering deterrence.

Senator KING. It's true, is it not, that allies are a tremendous force multiplier for our ability to have our policies respected and have our national security protected?

Lt. General RUDD. Senator, I think that's a—that's a great way to characterize it.

Senator KING. Thank you. I'll leave it at that.

Chairman COTTON. Senator Lankford.

Senator LANKFORD. Mr. Chairman, thank you, General. Thank you. Thank you for your decades of service already to the nation and for stepping up into this role. It's a tough role. We'll have lots of conversations in the days ahead, but they won't be in open settings like this. So, I think it would be helpful just for you to be able to articulate, what do you see as the principal threats that NSA needs to be focused in on? As you look around the globe and the issues that are out there in this open setting, what would you see as some of the principal threats?

Lt. General RUDD. Yeah, thanks, Senator. The—I—you know, my assessment aligns with our national security strategy and national defense strategy and how we articulate the priorities. Um, certainly from where I sit at USINDOPACOM day in and day out, China, Russia, North Korea, those are all critical threats that we pay attention to varying degrees of, uh, how we characterize those and how we prioritize those.

But I think it's pretty clear that those two state actors; certainly Iran continues to pose concern and threat to the nation. Um, I would couple alongside with that, violent extremists will be an infinite problem and I think increasingly narcotics and narco terrorists.

Senator LANKFORD. Okay, thank you. I want to follow up on Senator King's question to you as well. I have a similar question dealing with how we prepare for a response and a deterrent. You would have the unique responsibility of preparing a portfolio for the president if we have a cyberattack to be able to handle the president, here are the options.

Then he has to obviously make the decisions on that, but you'll have the role of actually handing that to him and saying here's a set of options. So, my question to you is, what do you plan to do to be able to prepare that set of options? What are your boundaries and limitations for the options that you would hand to any president?

And to say these are—these are the options that you have that fall within legal bounds, but that also are an effective deterrent.

Lt. General RUDD. Well, Senator, I think it speaks to what I would—how I would frame my priorities if confirmed for this and the initial approach. Obviously, making an assessment of where the organizations are at. But the first priority is speed. Second one is scale, the next one is innovation and then integration. We've got

to move as fast as we can to ensure that we've got the right technologies, the right capabilities and able to generate multiple options.

We need to be able to scale those options and not only just scaling within the size of the workforce as we—as we mentioned, relative to Cyber Command size, certainly there's an approach by the department to, uh, address that. But I think increasingly, we look at other partnerships as a means to scale.

Innovation, as I highlighted in my opening comments, that is an asymmetric advantage. And that is something we, as the United States, do better than anybody. So, we have to continue to harness innovation. As a leader, I would empower the workforce to explore, test, try, fail and figure out what's working.

And then ultimately, those capabilities and options have got to be integrated. They've got to be integrated across the joint force, they've got to be integrated in all domains and increasingly those options should be provided that enable us to integrate and pair those with other elements of national power.

Senator LANKFORD. OK, it's helpful. You've been a consumer of some of the intelligence information that's come across your desk and trying to be able to prepare for operations. I'm a consumer of intelligence documents as well. I have noticed over the past 10 years among some of our agencies that the documents and the analysis has gotten safer and safer and safer in the way that it's written.

Sometimes I read some analysis and I read it twice and think this doesn't say a thing. This is supposed to be telling me something, and I can't tell what this is trying to tell me because it's written so safe in it. One of the challenges that I would have before you is that NSA and with your analysts and folks as they're gathering SIGINT, to be able to make sure that the documents that are written and the reports that are done just say it bluntly. And that there is a sense of permission to say it frankly even at times and to not have a perception of being safe. I don't know if you've experienced some of the same things as you've read some of the intelligence documents in the past and some of the information reports, but I would encourage you to say it, frank, instead of safe, when it comes out of your analysts.

You don't have to respond to that one way or the other on it because you'll have to be able to read it. One last question that I had is a follow up on what the chairman was saying on 702. I think what I'm looking for, for anything is clarifying for the American people, the protections that have been put in place in statute to protect the American people that no one is spying on them, but also making it clear that this is an essential authority that we have to have to protect the safety of the Nation.

I'm looking for not just someone who will stand up and say, yes, we need that, but someone who will be an advocate for 702 to be able to explain it to people that need to hear it and to be able to articulate how the American people are actually protected by 702. Is that you?

Lt. General RUDD. Senator, if confirmed, certainly I would do everything I can to provide the best advice as we look to reauthorize or extend this, this critical authority.

Senator LANKFORD. Thank you. Thank you, Mr. Chairman.

Chairman COTTON. Senator Wyden.

Senator WYDEN. Thank you very much, Mr. Chairman. General, enjoyed talking with you and I think you know that one of the key issues for me in this position is basically adhering to what Ben Franklin was talking about, who said anybody who gives up their liberty to have security doesn't deserve either. And that's what we talked about, and I want to, as we talked about, get into some more, kind of specifics, not to like pin you down or something, but to get a sense of where you're actually headed on striking that balance that I think is so essential.

So, the administration, a number of months ago, secretly decided that its agents can break into homes without a judicial warrant. Basically, they said the Fourth Amendment doesn't matter anymore. So, here's the question a little bit broader than I talked about with you yesterday so we can see if we can find some common ground.

And that is, General, if you are directed to target people in the United States for surveillance, will you insist that there be a judicial warrant? And I would like to have a yes or no answer to this, and happy to have some context.

Lt. General RUDD. Yeah, Senator, I—again, I appreciate the opportunity to speak with you yesterday. Um, certainly this speaks—this question speaks to the mission of NSA and the authorities that it has been given. What I can tell you, Senator, is that if confirmed, I will absolutely commit to executing the foreign intelligence mission of the NSA in accordance with the authorities that it's been given and within all applicable laws.

Senator WYDEN. That respectfully though doesn't get close to what I'm talking about. I mean, that is about as vague as anything I've heard on—on the subject and, uh, it seems to me that unfamiliarity with basic constitutional rights is not something that can be accepted in this position. It's so, crucial and I continue to believe that what I described you as not mutually exclusive.

I think smart policies give you security and liberty, not so smart policies give you less of both. So, would you like to take another crack at perhaps telling me a little bit? As I said in the office, I'm interested in hearing, in your words, how you might deal with one of these issues. Not to spell it out in text and the like, but to get a sense of how you would strike this extraordinarily important issue in a sensible way.

Lt. General RUDD. Well, Senator, as again, as we discussed, I have utmost respect and commitment to the civil liberties that are outlined in the Constitution. I've sworn an oath several times throughout my career to uphold that Department.

Senator WYDEN. Let's move on so we can get some more questions. Do you believe that U.S. person searches of Section 702 collection should require a warrant except in emergencies, which has been largely the position of those who would like to find some common ground as we go forward? We would say, look, if somebody says this is a four alarm crisis for the country, they can get the information they need and come back and settle up later, which strikes me again as a constructive step. So, what are your thoughts

with respect to saying that you should have a warrant except in emergencies?

Lt. General RUDD. Well, Senator, that's—that's a topic that I'd need to look into and get a better understanding to give you a more fulsome and complete answer on that one. Again, what I would highlight though is supreme confidence that the men and women of the NSA are committed to protecting civil liberties and privacy of American citizens.

Senator WYDEN. Let me go a little bit further on the Greenland issue then you've gone today. Donald Trump's threat to invade Greenland is just one of many ways, in my view, we would damage NATO. You talked about the importance of intelligence relations and intelligence relationships. How concerned are you that these relationships could be damaged by the current tensions that we are talking about now with Greenland?

Lt. General RUDD. Senator, the alliances and partnerships that we rely on to execute our missions are absolutely critical.

Senator WYDEN. OK. Thank you, Mr. Chairman.

Chairman COTTON. Senator Rounds.

Senator ROUNDS. Thank you, Mr. Chairman, and General Rudd, first of all, thanks for your service to our country. I've appreciated our—our discussions already in armed services and then in my office as well. And I look—I have just—I look forward to supporting your nomination. But I thought this was an opportunity in a public discussion, different than what we normally do within a classified situation in which we can kind of share with the American people some of the concerns and some of the directions that we really have to go in order to, number one, gather good data to make good decisions, but also how we protect the American public from adversaries that have some pretty decent offensive cyber weapons systems that they're not afraid to deploy.

It—if we could for just a minute, let's talk a little bit about artificial intelligence and the need to be able to deploy it. I think some folks in—in the United States today have thought that, you know, if we have concerns about this, this new thing about being able to make decisions very, very quickly, which is what artificial intelligence allow sand to look at a lot of different data, uh, what happens if we were to simply say, you know what, we're just going to take our time in terms of deploying artificial intelligence in our, uh, data gathering, uh, or in our weapons systems.

Does that stop an adversary in any way, shape or form from integrating artificial intelligence as quickly as they can?

Lt. General RUDD. Senator, it wouldn't. And I think this is an area of—of competition that we have to accelerate in. It's—it's a critical capability that its adoption and integration into our joint warfighting functions and our intelligence collection has got to be adopted. That is what will enable us to maintain our advantage in all these—all these categories.

Senator ROUNDS. Would it be fair to say that in any warfighting situation, speed can make the difference between a life and death situation?

Lt. General RUDD. Senator, that's certainly my experience.

Senator ROUNDS. So, you've been around the horn a little bit. You've been with young men and women that have been in harm's

way. Would it be fair to say that if we deploy our tools faster than the bad guys can at a strategic level and we provide assistance to our young men and women in uniform at a faster pace, uh, and give them more information more quickly than what an adversary can, that we save lives?

Lt. General RUDD. Senator, I would agree with that. And again, the examples you give are, uh, very personal to me. I understand what it means to, uh, command forces in harm's way and what it means to make decisions quickly so that we protect our forces. But I would offer increasingly this is a strategic advantage, our decision making, our speed and our ability to outthink and outmaneuver the enemy before there's conflict is critically important as well, senator.

Senator ROUNDS. I'm going to bring this down now to a little bit more direct level, and we've talked a lot about 702 and about the need, and I fully support the continuation of 702 operations. A huge amount of the data that we're able to collect overseas, uh, to be able to give our war fighting teams an advantage is because of what we collect using 702. I know there's always a concern that we not collect any information on U.S. citizens.

But can you talk a little bit about what it means to a young man or a woman who is on the front lines and the ability for us to be able to know in advance what a bad guy is going to be doing near or around their areas and how critical it is that we take advantage of those opportunities to collect that data and not tie the hands of those individuals that collect it?

Lt. General RUDD. Senator, I would again offer my personal experience as a warfighter where I know that authority has enabled NSA to provide timely foreign intelligence to the warfighter that has saved lives.

Senator ROUNDS. Thank you. Let me go one step further now with regard to artificial intelligence. We've got to be able to collect as much data as we can as quickly as we can. And yet in order to do that, we can't simply rely on what we call government sources. We've got to be able to work with the private sector. A huge amount of the data that's collected, that's out there right now in terms of being able to make AI work even faster at the cutting edge is coming from private sector initiatives.u

Can you talk a little bit about how important it is to be able to integrate the private sector into our systems to make us faster than the adversaries?

Lt. General RUDD. Senator, it seems reasonable that that would naturally accelerate and enable scale. What I would also highlight is that as we do that, again, the same respect and safeguards for civil liberties and private data need to be adhered to.

Senator ROUNDS. Thank you. Thank you, Mr. Chairman.

Chairman COTTON. Senator Kelly.

Senator KELLY. Thank you, Mr. Chairman. Um, just like Senator Rounds, I wanted to talk about AI and FISA 702. I got one other topic. Just want to start by saying that I have legislation with Senator Warner and Cornyn and Lankford called the ENABLE IC Act, which is going to get these—get us moving faster on this.

And also an advanced AI Security Readiness Act which is going to help with something you talked about General Rudd, uh, the pri-

vate sector more involved here. So, I think we all agree that we need to move faster and innovate more and the world is moving credibly fast, especially with AI, and these tools that are being developed and these novel methodologies are incredible, but they also come with a lot of risk, especially when we're talking about a highly classified work environment.

Uh, and highly classified data. So, can you talk a little bit in more detail about how you're going to approach integrating AI and other tech tools into NSA systems that we currently have while guarding against the risk?

Lt. General RUDD. Senator, I would—I would offer on risk, the first way that we mitigate risk is to understand it. Where are the risks? Where do they exist? And then what do we need to do to ensure that we are continuously assessing that we've provided a solution to that. Within the realm of AI, obviously, the data is a key part of this, but then also equally important, a layer of cybersecurity around that.

So, how do you ensure that the data is authoritative? How do you ensure that it's feeding the right models? But equally important, coupled with that is the ability to protect that data. My understanding is that NSA has that responsibility. They're executing it very well. And certainly, Senator, if confirmed, it would be a high priority of mine to ensure that we continue to do so.

Senator KELLY. And, General, also, you know, one priority I think you're going to need to put somewhere near the top of the list, and I know, um, one of my colleagues brought up the election threat issue, but certainly AI being used by our adversaries against us in an election is going to be I think here in 2026 is going to be more significant than what we've ever seen before and certainly in 2028. On the FISA 702 question, um, we're going to have to have to reauthorize it here pretty soon, just a few months.

Um, I don't think the public understands what this is. I mean we're talking about something, I mean an acronym with a number and a letter after it and it just seems something that's, you know, out of reach for most people. Can you try to explain here in just about 30 seconds or so, why this should matter to the average American?

Lt. General RUDD. Senator, in as plain as language as I can put it is, first and foremost, it is the collection of foreign intelligence against non-U.S. persons who are located out the United States—outside of the United States. And again, what I've experienced in in my career is that this provides the warfighter, the decision maker, the ability to have critical insight into threats that enables decision making.

And again, we've talked about speed. Critical to speed is—is a deep understanding.

Senator KELLY. But for a family, hardworking American family, not—and they shouldn't have to pay much attention to this, how does it affect them? Like what are the consequences to them and their children let's say a few months from now if we did not reauthorize 702?

Lt. General RUDD. Well, Senator, again in my experience, it's quite simply, it saves lives.

Senator KELLY. Save lives, could it—could we be potentially talking about their lives, the lives of their family members, friends, coworkers?

Lt. General RUDD. Again, Senator, the lives of men and women in harm's way, but also threats to the—to the homeland, the United States. I would put that in the category of saving lives.

Senator KELLY. Yeah, and I agree with you, and I—and I think that is a key part of this. This is a—an authority that the intelligence community has, but the reason it has it is it keeps Americans safer. Not just the IC, not just DOD, not people that are regularly in harm's way, it results in safety for the American people.

Thank you, Mr. Chairman.

Chairman COTTON. Senator Budd.

Senator BUDD. Thank you, Chairman. General, thank you for your years of service. I enjoyed our conversation in the office a week or two ago. You know, we talked a lot about this morning and in that conversation in the office about the many hats of this role and you certainly had the experience to do that, but I understand that in a peacetime.

But let's say there's a—an invasion by China to Taiwan, um, and it's no longer peacetime, but it's a period of conflict. How do you balance the roles in a situation like that as best you can see it?

Lt. General RUDD. Well, Senator, it's a continuous assessment of the situation and where the balance lies between the two organizations and the capabilities that each brings to bear. Certainly on one side, you need deep insight into the threat, into the adversary, to understand. And then on the other side, you need to be able to deliver capabilities and options that would change the course even before conflict but if in conflict, certainly there's capability to bring to bear.

There's obviously a constant awareness and understanding of that. But I think the current construct puts us in a position that enables unity, of command unity, of effort to make decisions and over those two rapidly.

Senator BUDD. Thank you, general. You know, we've talked about your years of service and certainly a unique pathway to get to this point. So, congratulations for that. But, you know, this is a highly technical civilian organization at NSA, which it's different than a lot of what you've done before. Uh, tell us how you want to, and you think you will be adapting your military leadership experience to lead an organization like this?

Lt. General RUDD. Yes, Senator. The, uh—first of all, if confirmed, I look forward to this—this unique experience and challenge, uh, gaining a deeper understanding and appreciation of a largely civilian highly technical workforce. My career to-date is not without those experiences and opportunities perhaps, but this would definitely be a different one.

What I have always applied as a leadership principle to any organization, but certainly ones that are different or have different capabilities or different expertise, uh, is first a willingness to get in and learn as much as I can. But connect, connect with the workforce, connect on a personal level, get to know them. Certainly, I'm not going to get to know every single individual in the—in the agency, but get to understand their culture. The second piece is

what I just said, understand. And in doing the connection and understanding with the workforce, it enables a leader to best position themselves to empower, to enable, and to really harness what their capability—their incredible expertise is. And certainly if confirmed, I look forward to applying that with this organization.

Senator BUDD. Thank you, General. You know there's an executive branch policy where the NSA is prohibited from producing and disseminating finished intelligence. I found that interesting. And yet the agency NSA has some of the best cybersecurity expertise in all of the U.S. government. And it does, in fact, produce products that look and read a lot like finished intelligence.

So, is that a good policy?

Lt. General RUDD. Yes, Senator, that's something that I would want to take a look at and come back to you with a recommendation on.

Senator BUDD. That's my next question. So, you will commit to looking at that to see if that policy needs to be modified?

Lt. General RUDD. Senator, if confirmed, I'll look into it.

Senator BUDD. Thank you. Um, you spent a lot of time in the Indo-Pacific, where do you see opportunities to work with our—our partners like Japan, the Philippines and Taiwan, to build capacity in countering—against cyber threats and, um, how could we cooperate with them more?

Lt. General RUDD. Senator, we're doing it on a daily basis. Certainly there's opportunity to do more, but there's a very deliberate approach in campaign plan to working with our allies and partners. I think there's tremendous opportunity to do more certainly on the cyber front, and if confirmed, I would look—I would look forward to exploring those opportunities.

Senator BUDD. Thank you, General.

Chairman COTTON. Senator Gillibrand.

Senator GILLIBRAND. Thank you, Mr. Chairman. For nearly a decade, the intelligence community produced a steady stream of relevant intelligence on foreign threats to U.S. elections informing congressional policy makers. Will you commit to continuing to produce and disseminate intelligence reporting made available to Congress on foreign plans, intentions and activity targeting U.S. elections?

Lt. General RUDD. Senator, the electoral process is fundamental to our democratic values and Americans writ large. And I've committed throughout my career to serve to defend and uphold those values. Any foreign threat to the electoral process should be viewed as a national security concern. And, Senator, if confirmed for this, I commit to working with executive and legislative sides on this.

Senator GILLIBRAND. I appreciate that. In your responses to the Senate Armed Services Committee, you suggested very similar to that statement that U.S. election defense is currently better positioned than in the past given efforts with interagency partners which allows for the rapid sharing of threat intelligence. Under this administration, however, key elements of that interagency process have been entirely eliminated, as in the case of the FBI's Foreign Influence Task Force, or been paralyzed from funding cuts and rollbacks of information sharing duties.

Do you believe that there's still an effective interagency for you to engage with?

Lt. General RUDD. Well, Senator, if confirmed for this role, I would look forward to being part of whatever the construct exists. Certainly, again, throughout my career, I've seen—I've seen and I've been a part of a number of interagency efforts. So, if confirmed, I look forward to being part of this.

Senator GILLIBRAND. Okay. Several years ago I led the creation of the DOD Cyber Service Academy Scholarship program, which creates a cleared and trained workforce pipeline. These are for non-military roles appropriate for NSA, CIA and other civilian positions. Since then, I've worked with my colleagues to continue to improve this program and expand the number of scholarships.

What value do you see in this type of program and how would increasing the number of scholarships benefit NSA's work? If confirmed, do I have your commitment to work with me on this project?

Lt. General RUDD. Senator, I'd certainly like to learn more about this. But I—the way you describe this concept certainly seems like a—an avenue that could be explored to enhance and expand the scale of the workforce, certainly an opportunity to generate talent for the workforce. And so, Senator, if confirmed, I look forward to learning more about this.

Senator GILLIBRAND. Yeah, and when we created it, it has up to 1,000 slots a year, but we have not done a good job in telling our high schools around the country that these scholarships are available. And so, we have not had sufficient applications. In the last few years it's been in the hundreds, not in the thousands. And so, all slots are not being filled.

Um, we've also worked to get more schools signed up. There's over 600 schools across the country that have signed up for this ROTC type program as long as they have the curriculum that our security and intelligence teams need across the DOD and across the Intel Community. So, I would like your commitment also to work with us in making sure high school students around the country know about this and that all your services know that they can find great graduates through this program.

Lt. General RUDD. Senator, again, I look forward to learning as much as I can about this and supporting it as able.

Senator GILLIBRAND. Thank you. Last year, DNI Gabbard fired over 100 intelligence officers deemed to be misusing the chat platform hosted by the NSA on Intelink. These officers were alleged to have misused these systems, in some cases with valid allegations of inappropriate conduct and others potential for discriminatory reasons.

You've answered to many of the members on this panel about your review and judgment with regard to the use of AI platforms on NSA systems. What is your perspective on making sure these systems are not misused to harass or target other service members or intelligence personnel?

Lt. General RUDD. Yes, Senator, I appreciate that concern. Certainly the responsibility of any leader of any organization is to safeguard the workforce and ensure that there's compliance within how

we use the tools and systems to accomplish the mission. And if confirmed for this role, I would pledge to continue that.

Senator GILLIBRAND. Thank you. Thank you, Mr. Chairman.

Chairman COTTON. Senator Young.

Senator YOUNG. General Rudd, good to see you again. I enjoyed our visit in the office, appreciate your answers to my many questions. You noted in your committee questionnaire before this hearing that one of your priorities for improving NSA's coordination with the rest of the IC will rely on fostering interagency training, exercises and experimentation.

Can you unpack this for the committee, please?

Lt. General RUDD. Well, Senator, I think the way that we build connective tissue through organizations, not only within the department, but to the point of the question within the interagency, is through repetitions and sets, you know, whether it be training, training exercises, tabletop exercises. Those are ways that we exercise the muscle, the connective tissue, of organizations and enhance the way we work together.

Senator YOUNG. Thank you. You also noted in your questionnaire a desire to leverage commercial innovation. We hear about this a lot. We need to hear about this. But beyond the obvious role for the commercial tech sector to play in making NSA more effective, more cutting edge, can you speak to how you might seek to increase opportunities for outside experts to come in to lead on emerging tech or economic competition to enhance your analytical capabilities?

Lt. General RUDD. Yes, Senator, I think that's a critically important effort and certainly we need to look at every opportunity to expand our expertise. Again, CYBERCOM and NSA have tremendous expertise, talent, probably the best in the world at what they do and we have to continuously find those opportunities where we learn, enhance, never be complacent that what we're doing is sufficient, especially in—in the world of technology that's moving so fast.

And so much of the commercial sectors moving out at a very fast pace.

Senator YOUNG. General, can you describe the role you see for NSA in helping shepherd safe and effective U.S. government and IC artificial intelligence technologies, especially through the AI Security Center?

Lt. General RUDD. Yeah, thanks, Senator. That's the example I was going to mention, the effort underway that uses Intel driven understanding to make recommendations and solutions to enhance the security around AI, not only within the department, the organization, but with our commercial partners where applicable as well.

Senator YOUNG. Will you commit to working with this committee and identifying any shortfalls, whether it's of resources, authorities or prioritization for NSA and the ICs development and use of AI?

Lt. General RUDD. Senator the—the role of any commander, leader, director is certainly to identify what those are. And if confirmed, I do commit to that.

Senator YOUNG. OK. Thank you, Chairman.

Chairman COTTON. Senator Ossoff.

Senator OSSOFF. Thank you, Mr. Chairman, and General, thank you for your career of service to the United States and congratula-

tions on your nomination to this important post. Before I engage with you, I just want to note for the committee that my constituents in Georgia, and I think much of the American public, are quite reasonably alarmed and asking questions after the Director of National Intelligence was spotted bizarrely and personally lurking in an FBI evidence truck in Fulton County, Georgia yesterday.

And so, I encourage all of us on a bipartisan basis to pursue the facts as swiftly as possible to understand whether the Office of the Director of National Intelligence is straying far outside of its lane. At unrelated—I regret to share my observation that the president at this point is clearly using federal law enforcement in order to pursue personal vendettas. That has nothing to do with you and your career to-date, nor is it something for which I hold you accountable or would expect you to explain, but it is a well-known fact, and it quite reasonably, given the immense surveillance capabilities of the National Security Agency, raises the concern that there might be some abuse of the NSA's authorities.

And so, my question for you is that if there is some alteration or withdrawal of current prohibitions, administrative prohibitions, on surveillance targeting Americans, for example, in Executive Order 1233, PPD–28, USSID 18 or otherwise, will you promptly inform this committee with our oversight responsibilities of such a change?

Lt. General RUDD. Senator, I will pledge, if confirmed, to ensure that the NSA executes its mission within the authorities and all applicable laws and that I will execute the duties of this position that enables this committee to exercise its oversight responsibilities.

Senator OSSOFF. General, I appreciate the answer and I want you to think a little bit more deeply about the question and consult with your team and follow-up with more precision for the record. Because the challenge I'm identifying is that you may be asked to do things that are manifestly unethical and improper, but following some alteration of present administrative policy, may indeed be lawful.

And this committee needs to know if such administrative policies, which currently protect American civil liberties but are not in statute, are changed. And my view would be that under existing law, anyone in the seat that you hope to hold would have a statutory obligation to inform this committee of any such change.

So, I hope to get some more detail beyond boilerplate on that for the record. You will also be taking this post, General, if confirmed. So, can I get a commitment that you will respond with a more fulsome answer for the record please, general?

Lt. General RUDD. Senator, I look forward to looking into that topic and responding to you.

Senator OSSOFF. Thank you. If confirmed, you'll take this post after a series of events that suggest a crisis for information security and operational security practices in the federal government. You had the Secretary of Defense inadvertently text strike details to a national political reporter, including time over target for U.S. aircrews before those U.S. aircrews had launched into hostile enemy airspace.

Multiple major news outlets were reportedly aware of the imminent raid targeting Maduro in Venezuela before the raid was executed. This week, here's a headline from Politico, Trump's acting cyber chief uploaded sensitive files into a public version of ChatGPT. NSA has a crucial role supporting information security, cryptographic integrity and best practices across the federal government.

How will you and your role constructively address these many failures and the broader problem of information security failures in the federal government?

Lt. General RUDD. Senator, I recognize the critical role that NSA plays in this space and certainly, if confirmed, I pledge to ensure that it continues to execute its mission to its fullest.

Senator OSSOFF. Thank you, General.

Chairman COTTON. Senator Cornyn.

Senator CORNYN. Welcome, General, and congratulations on your nomination and I appreciate the ability to talk to you, although because of weather concerns, it was on the phone. But, um, you obviously have a lengthy record of distinguished service to our nation and I look forward to supporting your nomination. In your current capacity as deputy commander of INDOPACOM, do you occasionally have to talk to a lawyer or maybe more than one lawyer?

Lt. General RUDD. Senator, there is a very talented legal team at USINDOPACOM.

Senator CORNYN. Yeah, it seems like a blessing or a curse, just speaking as a recovering lawyer myself, but it seems like you can't—you can't make a move without consulting legal authorities. And so, do you happen to know how many lawyers are at NSA CYBERCOM?

Lt. General RUDD. Senator, I don't know that.

Senator CORNYN. Yeah, it's a whole bunch, and they're very talented.

Lt. General RUDD. I would guess there is and I would—I would expect that they would be.

Senator CORNYN. Will you be consulting with them on issues like, uh, let's say, 702, Section 702 FISA?

Lt. General RUDD. Senator, I would expect to consult with the legal experts at both CYBERCOM and NSA on a whole host of issues to ensure, again, the execution of that mission set is done within the authorities consistently and that we're never outside the bounds of that.

Senator CORNYN. I have—I have no doubt about that. The Judiciary Committee also has jurisdiction over the 702 issue. But, um, I, like others, believe that it's absolutely—absolutely essential authority, but there's a phenomenon in Washington, DC, where, uh, certain narratives take root, which have no basis in fact.

And, I just want to clarify a few things. First of all, one of the reasons why 702 had come under suspicion is because of its abuse in the case of Carter Page, but that was a Title I, 7—of 702, which is targeting an American citizen. In this case, an alleged agent of a foreign power. That law is not subject to any reauthorization.

It doesn't expire. But just in terms of 702, Title VII, which is what, uh—so, what we're talking about. I know there's a line of questioning by one of our—one of the panel talking about targeting

U.S. persons. You can't target a U.S. person without a warrant, and that's under Title I not on—on under Section 702. But you understand that, um, 702, Title VII, um, is—uh, addresses only foreigners abroad.

Is that—is that your understanding? It's a foreign intelligence surveillance.

Lt. General RUDD. Senator, that's my understanding that 702 is focused on foreign intelligence against non-U.S. persons outside the United States.

Senator CORNYN. And it's an invaluable resource, correct?

Lt. General RUDD. In my experience it is, Senator.

Senator CORNYN. And I'm sure you, like all of us, are very attuned to the balance between national security demands and privacy of American citizens. But in this case, this is focused solely on people overseas. So, there is no targeting of American citizens, of course, unless you have a—unless you have a warrant and you got to show up in front of the Foreign Intelligence Surveillance Court and prove that you are entitled to that warrant.

But we're not talking about that here. But here again in DC, it seems like the—whoever has the—that you have this phenomenon of competing narratives, and I read a long time ago that whoever has the best narrative wins in the debates here in Washington, DC, whether or not they're based on facts.

Another issue that's come up, and let me just ask, and I mean this with all due respect, you have an incredible record, but you are not a lawyer by training, are you sir?

Lt. General RUDD. No, Senator, I'm not.

Senator CORNYN. You're unburdened by that—by that credential. So, that's why you're going to be talking to your lawyers before you make any decision. But there's also this false narrative that lawfully collected intelligence that somehow you ought to be able to you ought to have to go out and get a search warrant in order to search what you've already lawfully collected.

And of course, intelligence is prospective. Law enforcement is retrospective based on trying to solve a crime. But do you have a—are you prepared today, or would you like to give it some thought and maybe we can engage further on whether or not a warrant should be required to query lawfully collected intelligence?

Lt. General RUDD. Senator, that's certainly something I'd like to take a deeper look at.

Senator CORNYN. Thank you. My time is up. Thank you.

Chairman COTTON. Thank you, General Rudd, for your testimony here today. For the benefit of members, and General Rudd, it's my intention to hold a committee vote on your nomination as soon as possible. Therefore, for planning purposes, any senator who wishes to submit questions for the record after today's hearing, please do so by noon tomorrow.

General Rudd, I trust that you'll be equally prompt with your answers so we can move your nomination forward as quickly as possible. Thank you all, the hearing is adjourned.

(Whereupon the hearing was adjourned at 11:35 a.m.)

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: Joshua Monroe Rudd
   OTHER NAMES USED: Josh

2. DATE AND PLACE OF BIRTH: 4 Dec 1971 / Van Nuys, CA
   CITIZENSHIP: United States Citizen

3. MARITAL STATUS: Married

4. SPOUSE'S NAME: Ansley Denka Rudd

5. SPOUSE'S MAIDEN NAME IF APPLICABLE: Denka

6. NAMES AND AGES OF CHILDREN:

NAME	AGE
REDACTED	

7. EDUCATION SINCE HIGH SCHOOL:

INSTITUTION	DATES ATTENDED	DEGREE RECEIVED	DATE OF DEGREE
Furman University	1989-1993	BA Political Science	May-93
Naval War College	2007-2008	MA National Security & Strategic Studies	Jun-08
Duke University	2014-2015	Senior Service College Fellowship	Jun-15

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
US Army	Platoon Leader of 608th Ordnance Co, 13th Corps Support BN	Fort Benning, GA	June 94-May 95
US Army	Platoon Leader of 598th Maintenance Co, 13th Corps Support BN	Fort Benning, GA	June 95-Jul 96
US Army	Logistics Officer, Ranger Training BDE	Fort Benning, GA	Aug 96-Oct 98
US Army	CDR of SF, A Co, 3rd BN, 7th Special Forces Group (AB)	Fort Bragg, NC	Nov 99-Jun 02
US Army	CDR of SF, C Co, 3rd BN, 7th Special Forces Group (AB)	Puerto Rico/Fort Bragg, NC	Jul 02-Apr 04

US Army	Troop Commander, USASOC (AB)	Fort Bragg, NC	May 04-Jun 07
US Army	Student, Naval War College	Newport, RI	Jul 07-Jun 08
US Army	Deputy Ops Officer, Group, USASOC (AB)	Fort Bragg, NC	Jul 08-Jun 09
US Army	Squadron Commander, USASOC (AB)	Fort Bragg, NC	Jul 09-Jun 11
US Army	Chief, Current Ops Division, Joint Special Ops Command	Fort Bragg, NC	Jul 11-Jun 13
US Army	Deputy Commander (Ops), Group, USASOC (AB)	Fort Bragg, NC	Jul 13-Jun 14
US Army	Senior Service College Fellowship, Duke University	Durham, NC	Jul 14-Jun 15
US Army	Commander, Group, USASOC (AB)	Fort Bragg, NC	Jul 15-Jun 17
US Army	Commander, Joint Interagency Task Force - NCR	Washington, DC	Jul 17-Jun 18
US Army	Deputy Commanding General, 1st SF Command (AB)	Fort Bragg, NC	Aug 18-Jul 19
US Army	Deputy Commanding General (Ops), 25th Infantry Div	Schofield Barracks, HI	Jul 19- Jul 20
US Army	Commander, Special Operations Command Pacific	Camp H. M. Smith, HI	Aug 20-Jul 22
US Army	Chief of Staff, United States Indo-Pacific Command	Camp H. M. Smith, HI	Jul 22-Sep 24
US Army	Deputy Commander, United States Indo-Pacific Command	Camp H. M. Smith, HI	Sep 24-Present

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).

N/A

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

My comprehensive background in national security, military operations, and specialized intelligence is in direct alignment with the strategic objectives of the 2025 National Security Strategy, specifically concerning homeland defense, deterrence, capability integration, and operational readiness. Throughout pivotal leadership roles within the Indo-Pacific theater, the U.S. Army, the Joint and Special Operations, I have possessed the unique vantage point of being both a consumer of and a contributor to the intelligence and operational capabilities of the NSA and Cyber Command. This front-line, war fighting perspective has bestowed upon me a profound understanding of the complex interplay between the resources, talent, technology, authorities, and operational considerations that drive the missions of both organizations.

Below is a summary of expertise acquired through key leadership roles:

Deputy Commander, U.S. Indo-Pacific Command

- Managed the interagency portfolio to integrate military capabilities from joint services with interagency efforts, including economic, diplomatic, information-based capabilities, and the U.S. industrial base and innovation. Focused on deterring China and maintaining regional stability. This portfolio is critically dependent on accurate, timely and thorough intelligence products, I have enhanced the relationship across the USINDOPACOM enterprise with the Intelligence Community's (IC) various resources, inclusive of USCYBERCOM and NSA.
- Directed all-source intelligence and cyber capabilities to carry out sensitive command missions, using delegated authorities from Commander, U.S. Indo-Pacific Command.
- Leveraged whole-of-government capabilities to align military operations with diplomatic, economic, and information strategies, supporting the Strategy's emphasis on burden-sharing and multi-domain deterrence.

- Partnered with U.S. industry to advance technological innovation and strengthen the defense industrial base, consistent with the Strategy's focus on economic security and technological superiority.

Chief of Staff, U.S. Indo-Pacific Command

- Directed strategic planning, operations, and critical coordination of interdependent functions from all the joint services and partners and allies, for the Indo-Pacific region, ensuring alignment with national security objectives.
- Coordinated multi-domain operations to address regional challenges, supporting the strategy's focus on deterring adversaries and maintaining regional stability.
- Leveraged advanced intelligence and operational tools to maintain decision advantage, consistent with the Strategy's emphasis on technological innovation.

Commander, Special Operations Command Pacific

- Led Special Operations units across the Indo-Pacific, addressing regional challenges such as irregular warfare, counterterrorism, foreign internal defense, influence operations, sensitive activities, and partner capacity-building to achieve deterrence, and maintain a free and open Indo-Pacific.
- Drove intelligence requirements for Special Operations Forces and conduct coordination to ensure timely, operational intelligence sharing with foreign partners and whole of U.S. Government, leveraged Special Operations Forces access and placement to optimize collection and IC capabilities.
- Strengthened alliances and partnerships to deter adversaries and maintain a free and open Indo-Pacific, consistent with the National Security Strategy's regional priorities.
- Integrated land, sea, air, space and cyber capabilities to address complex threats, supporting the Strategy's emphasis on deterring military threats.
- Operations in multiple domains directly contributed to enhancing NSA efforts.

Deputy Commander, 1st Special Forces Command

- Oversaw the training, equipping, and deployment of Army Special Forces military, civilians and contractors to address global and regional security challenges. Oversaw the innovation of capabilities of a diverse technical, kinetic and non-kinetic profile, building critical relationships with Silicon Valley and the federally funded research and development enterprise.
- Ensured Army Special Forces were prepared to deter and win conflicts, train and advise mission partners and allies.
- Led meaningful engagement with Ally and Partner Special Operations joint military leaders, strengthening the interoperability and increasing the capacity of the U.S. interests.

Commander, Joint Interagency Task Force for the National Capital Region

- Led a critical homeland defense mission, integrating military services, the Intelligence Community, and interagency, ensuring coordination across the whole of government. This mission heavily depended upon IC collection and reporting at the tactical and operational levels, drawing upon multiple sources.
- Responsible for addressing external foreign threats, providing situational awareness, continuity of government operations, defense support of civil authorities during emergencies, joint command and control.

Commander, Group, USASOC (Airborne)

- Directed national mission operations to achieve strategic effects, focusing on counterterrorism and high-value target missions. Delivered decisive outcomes in support of national security priorities.
- Employed cutting-edge operational and tactical intelligence to inform operations, ensuring mission success and alignment with the Strategy's focus on technological superiority. Responsible for leveraging the

capability and capacity of the entire U.S. IC to support critical national priority missions, from targeting to assessment.

Current Operations Chief/J3, Joint Special Operations Command

- Directed operational planning and execution (both Title 10 and Title 50) for joint and coalition global special operations missions, including counterterrorism and crisis response. Led global operations to neutralize threats to the U.S. homeland and U.S. interests, aligning with the National Security Strategy's focus on preventing adversarial dominance.
- Built cohesive and lethal teams across the whole of U.S. government. Worked closely with intelligence and defense partners to ensure mission success, supporting the Strategy's emphasis on burden-sharing.

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).

Defense Superior Service Medal (with 3 Bronze Oak Leaf Clusters)
Legion of Merit (with 2 Bronze Oak Leaf Clusters)
Bronze Star Medal (with 2 Bronze Oak Leaf Clusters)
Defense Meritorious Service Medal (with 2 Bronze Oak Leaf Clusters)
Meritorious Service Medal (with 1 Bronze Oak Leaf Cluster)
Army Commendation Medal
Joint Service Achievement Medal (with 1 Bronze Oak Leaf Cluster)
Army Achievement Medal (with 1 Bronze Oak Leaf Cluster)
Combat Infantryman Badge
Master Parachutist Badge
Military Free Fall Jumpmaster Parachutist Badge
Special Operations Diving Supervisor Badge
Ranger Tab
Special Forces Tab
Pathfinder Badge
Senior Service College Fellowship, Duke University

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
Military Officers Association of America (MOAA)	N/A
Association of the United States Army (AUSA)	N/A
Special Forces Association (SFA)	N/A

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?

Yes

EVENT	LOCATION	DATES
AFCEA TECHNET	Honolulu, HI	30 October 2025
Indo-Pacific Irregular Warfare Symposium	Bangkok, Thailand	20 August 2025
SOF Week	Tampa, FL	22 May 2025
Information Operations & Electronic Warfare Symposium	Honolulu, HI	18 October 2023
AFCEA TECHNET	Honolulu, HI	01 November 2022

PART B - QUALIFICATIONS

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

My 32-year career is first and foremost as an experienced leader of our professional armed forces and civil servants. I have the experience as a dedicated warfighter and joint force commander whose mission is fundamentally reliant upon the critical intelligence and operational capabilities of the National Security Agency and U.S. Cyber Command. The Director of the NSA is charged with the dual responsibility of generating decisive signals intelligence (SIGINT) for our nation's leaders while simultaneously securing our most vital national security systems. Having been an operator at the receiving end of these outputs, I possess an intimate, first-hand appreciation for how intelligence must be tailored, delivered, and protected to be effective at the strategic, operational, and tactical levels, giving me a sophisticated, working knowledge of the agency's most critical mission. As an operator, I also have a strong understanding of risk and risk mitigation, not only to preserve intelligence sources and methods, but also to protect U.S. forces and missions.

Simultaneously, the leadership of U.S. Cyber Command demands a commander who not only comprehends its mission but also possesses a deep, practical understanding of its synergy with the broader national security ecosystem. Leading highly trained, cohesive forces against the rapidly evolving, technologically advanced threats of the modern era have endowed me with the practitioner's insight required to command CYBERCOM. This experience has instilled in me the ability to bring together disparate people, partners, and technologies to achieve unified, mission-critical outcomes against adversaries who operate with increasing speed and sophistication.

This is a pivotal moment requiring a leader committed to speed, innovation, effects, and legally and ethically grounded operations. I offer a proven track record of leading through innovation, demanding results, and ensuring transparent, ethical conduct in the most demanding and consequential situations. I am humbled by this opportunity and prepared to lead the people, partners, and technologies of these two vital organizations to defend the homeland, deter our adversaries, and ensure our nation's decisive advantage by providing its leaders with legally-sound options.

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, 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 ADMINISTRATION AND EXECUTION OF FEDERAL LAW OR PUBLIC POLICY.

No

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, PLEASE EXPLAIN.

N/A

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.

N/A

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.

None

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 OF ALL SECURITIES, REAL PROPERTY, PARTNERSHIP INTERESTS, OR OTHER INVESTMENTS OR RECEIVABLES WITH 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
None		

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
None		

30. 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

31. LIST THE SPECIFIC SOURCES AND AMOUNTS OF ALL INCOME YOU 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.)

REDACTED

32. 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

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

REDACTED

34. 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 SUCH PROCEEDING.

No

35. 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

36. 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

37. 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?

REDACTED

PART E - ETHICAL MATTERS

38. 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

39. 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

40. 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

41. 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

42. 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

43. 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 TO ONLY CONSIDER PROCEEDINGS AND LITIGATION THAT OCCURRED WHILE YOU WERE AN OFFICER OF THAT BUSINESS.)

No

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

No

PART F - SECURITY INFORMATION

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

No

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

No

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

N/A

PART G - ADDITIONAL INFORMATION

48. 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.

Congress' responsibility to provide oversight of the executive branch is a foundational element of American democracy and essential to the performance of its constitutional functions. The Intelligence Committees are tasked with the important duty of overseeing U.S. intelligence activities, ensuring that the IC operates in compliance with the law, which in turn enables the public to have trust and confidence in its work. To ensure the Intelligence Committees have the necessary information to carry out their authorized responsibilities, it is the obligation of the Director of the NSA to keep the Intelligence Committees fully and currently informed of all of NSA's intelligence activities consistent with the constitutional and statutory obligations of the Executive Branch.

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

The Director of the National Security Agency (NSA) is responsible for leading the agency's signals intelligence (SIGINT) collection and dissemination efforts, as well as helping to protect the nation's intelligence and military networks. As a foreign intelligence agency, the NSA collects sensitive communications, data, and weapons systems intelligence from adversaries to provide indications, warnings, and insights critical to U.S. national security and homeland defense. The Director ensures the protection of U.S. national security systems, shares threat intelligence and mitigations to deter threats in the cyber domain, and provides timely intelligence support to combatant commands as a combat support agency. Additionally, the Director contributes to strategic intelligence assessments that inform U.S. policymakers, including the President, while ensuring the delivery of tactical, operational, and strategic intelligence to a diverse range of customers in a timely, effective, and legal manner.

The Director also oversees the Central Security Service (CSS), which integrates the cryptologic activities of the Army, Navy, Air Force, Marines, Coast Guard, and Space Force with the NSA.

The Director also serves as the Commander, U.S. Cyber Command and executes its combatant commander duties as defined by law and policy.

AFFIRMATION

I, **JOSHUA M. RUDD**, DO SWEAR THAT THE ANSWERS I HAVE PROVIDED TO THIS QUESTIONNAIRE ARE ACCURATE AND COMPLETE.

09 JAN 2026
(Date)

JOSHUA M. RUDD SIGNATURE REDACTED

(SEAL)
AUTHORITY: 10 USC 936 & 1044A
Commission Indefinate Until Retirement
or Resignation

NOTARY SIGNATURE REDACTED

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.

JOSHUA M. RUDD SIGNATURE REDACTED

Date: 09 JAN 2026

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

Additional Prehearing Questions for

Lieutenant General Joshua M. Rudd

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 Director of the National Security Agency (NSA) and Chief of the Central Security Service (CSS) leads the nation's premier cryptologic organization and is responsible for two core missions of vital importance to our national security: signals intelligence (SIGINT) and cybersecurity. Under the authority of the Director of National Intelligence and the Under Secretary for Intelligence & Security, the Director oversees the SIGINT mission to produce critical foreign intelligence that provides decision advantage to our nation's leaders and warfighters. Concurrently, the Director leads the cybersecurity effort to prevent and minimize risks to our National Security Systems and the Defense Industrial Base (DIB). The Director also drives innovation in cryptography and advanced technologies to maintain the United States' advantage over adversaries.

QUESTION 2: Currently, the position of DIRNSA is dual-hatted with the Commander of U.S. Cyber Command.

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

Splitting the dual hat does not change the roles and responsibilities of the Director, NSA nor Commander, U.S. Cyber Command (USCYBERCOM). NSA and USCYBERCOM are separate organizations with distinct though related roles and missions with unique authorities, resourcing, and oversight. However, they share a single, overlapping, and inseparable operating environment, and the dual hat provides a unified commander responsible for the mission outcomes of both. This arrangement allows coherent priority setting, capability integration, and mission execution that best protects sensitive relationships and equities while ensuring the speed and agility to meet the challenges of a rapidly changing and dynamic technological and threat environment.

b. Which roles and responsibilities as the Commander of U.S. Cyber Command would be affected by a cessation of the dual-hat regime?

The cessation of the dual-hat construct could complicate efforts to align strategic objectives and resource allocation. Without unified leadership, there is a risk of misalignment between intelligence priorities and operational requirements, potentially leading to inefficiencies in resource utilization and mission execution. The dual-hat arrangement has historically provided a singular vision that ensures both organizations are working toward shared goals, and its removal could fragment this cohesion.

While cessation of the dual-hat leadership construct might offer some benefits, such as allowing each organization to focus more narrowly on its specific mission set, it also introduces risks that could hinder the Commander's ability to effectively lead USCYBERCOM. These risks include slower operational pace, reduced transparency, increased latency, and potential misalignment of strategic objectives—all of which could undermine the ability to protect the U.S. homeland, deter adversaries, and maintain technological superiority in the SIGINT and cyber domains.

c. What in your view are the positive and negative aspects of a dual-hat regime? Please provide details in supporting your position, and include assessments of structure, budgetary procedures, and oversight of NSA, as well as U.S. Cyber Command.

NSA and USCYBERCOM have distinct but complementary missions in the cyber domain. These responsibilities for intelligence and defense must be coordinated. As USCYBERCOM continues to mature, its relationship with NSA should be continuously evaluated to ensure each organization's primary mission is executed with maximum effectiveness and efficiency. From my perspective as the Deputy Commander of U.S. Indo-Pacific Command (USINDOPACOM), the ability to fuse SIGINT and multi-domain operations at speed is a decisive advantage. I also have firsthand warfighter and joint commander experience from U.S. Central Command (USCENTCOM), U.S. Africa Command (USAFRICOM), and USINDOPACOM that make a compelling argument for the advantages in warfighter support this integrated dual-hat approach provides. I understand the Dual Hat Study led by General Dunford affirmed this arrangement is in the best interest of the nation. The missions are inextricably linked, and if confirmed, I would be committed to ensuring the unity of effort this arrangement provides continues to deliver

results for the Joint Force. I am equally committed to the continuous assessment of the dual-hat advantages and disadvantages.

From a budgetary perspective, if confirmed, I would operate on the clear principle that all funds must be used for their appropriated purpose. While I am not familiar with the specific accounting details today, I understand the study confirmed clear processes are now in place to ensure accountability and cost reimbursement between the two organizations. Enforcing those agreements rigorously would be a key priority for me.

I commit to learning more about ways that the dual-hat status can foster more speed and agility between the two organizations, as it supports the warfighter with inextricably linked SIGINT, cyber domain capabilities, and protection.

QUESTION 3: If confirmed, how will you balance the four discrete responsibilities you will have to execute as DIRNSA, the Chief of the Central Security Service, the Commander of U.S. Cyber Command, and the National Manager for National Security Systems?

If confirmed, I intend to balance these discrete responsibilities by leveraging my extensive experience in integrating complex multi-domain global operations and leading multidisciplinary teams to deliver outcomes for the nation. To ensure unity of effort, I will maintain a strategic balance between the distinct roles, ensuring that each mission is executed with maximum effectiveness and efficiency. I will build and strengthen relationships across the military services, allies and partners, the interagency, the defense industry, and Congress.

Additionally, if confirmed, I will rigorously manage resources and ensure the well-being and readiness of our civilian, military and contractor workforces.

QUESTION 4: Please describe which of those roles you believe is most important, and why. Please provide supporting details in your answer.

As the current Deputy Commander of USINDOPACOM, I believe that all the roles listed—Director of the NSA, Chief of the CSS, Commander of USCYBERCOM, and National Manager for National Security Systems—are equally important and interconnected. The Director of the NSA focuses on SIGINT and, as National Manager for National Security Systems, the cybersecurity of our most critical systems, while the Commander of

USCYBERCOM leads cyber operations to defend the nation. The Chief of the CSS bridges NSA capabilities and the operational needs of the military services. Effective integration and collaboration across these roles are essential for protecting and advancing our national interests. I would strive to balance and strengthen each of these roles to ensure we have a comprehensive and robust national security posture, if confirmed.

QUESTION 5: How well do you think the NSA has performed recently in each of these missions?

In my role as the current Deputy Commander of USINDOPACOM, I believe NSA performs very effectively in supporting the Command's priorities. If confirmed, I would assess NSA's performance across all its mission sets and commit to ensuring that each of these missions are executed with maximum impact moving forward.

QUESTION 6: Please describe the specific experiences you have had in your professional career that will enable you to serve effectively as DIRNSA. In addition, what lessons have you drawn from the experiences of current and former DIRNSAs?

I have been privileged to serve for over three decades in leadership roles spanning the Joint Force, with extensive experience in the Indo-Pacific theater. My career has provided me with a deep, mission-driven understanding of the operational and strategic challenges we face, particularly concerning China.

As the current Deputy Commander of USINDOPACOM, I have been responsible for integrating operations across all domains—including cyberspace—to reinforce deterrence and prepare to fight and win if deterrence fails. This role has given me firsthand insight into the operational and intelligence needs of the warfighter and the critical importance of integrating SIGINT and synchronizing cyber effects with kinetic and non-kinetic capabilities. My prior leadership positions in U.S. Special Operations and in joint task forces have honed my ability to lead multidisciplinary teams, manage complex operations, assess risk, and build the strong relationships with allies and partners that are essential to prevailing in strategic competition. These experiences have prepared me to lead the men and women of NSA and ensure their world-class capabilities and talent are fully leveraged and integrated to support our national security objectives.

QUESTION 7: If confirmed as DIRNSA, what steps will you take to improve the integration, coordination, and collaboration between NSA and the other IC agencies?

As Director of the NSA, this will be a top priority to enhance mission effectiveness and ensure a unified approach to national security challenges.

To achieve this, I will take the following steps, if confirmed:

1. **Assess.** Assess the current strengths and weaknesses of interagency communication challenges—specifically, by looking at what codified forums address cross-cutting issues such as intelligence collection, processing, dissemination, cybersecurity, counterterrorism, and foreign influence operations.

2. **Seek enhanced data sharing and interoperability.** Evaluate current policies, practices and technologies that foster intelligence integration. Where necessary, enhance and implement secure, timely, and seamless sharing of intelligence data across IC agencies. This includes leveraging technologies, such as artificial intelligence (AI), to improve data integration and analysis while ensuring compliance with legal and ethical standards.

3. **Foster interagency training, exercises and experimentation.** Develop and oversee interagency training and simulation that bring together intelligence talent from NSA and the intelligence enterprise to enhance build trust, improve coordination, and enhance mission readiness. These initiatives will focus on real-world scenarios that require interagency collaboration, such as cyber defense and crisis response.

4. **Leverage commercial innovation.** Create opportunities for NSA and IC agencies to co-develop tools, technologies, and methodologies that address shared challenges. Where appropriate leverage performing industry partners, and advanced academic research into innovation hubs and accelerators to drive rapid advancements in intelligence capabilities.

By implementing these steps, I will ensure NSA is fully integrated into the broader IC framework, enabling more effective collaboration, reducing duplication of effort, and enhancing the collective ability to address complex national security challenges staying ahead of our threats.

If confirmed, I will continually evaluate the NSA's relationships with other IC partners to ensure the most effective mission execution.

QUESTION 8: If confirmed as DIRNSA, how will you ensure that the tasking of NSA resources and personnel to support U.S. Cyber Command does not negatively impact NSA's ability to perform and fulfill core missions?

If confirmed, I will continuously evaluate the relationship between the two agencies while maintaining the unity of effort provided by the dual hat structure. My goal would be to optimize the complementary but distinct roles of both organizations while preserving NSA's' world-class intelligence and cybersecurity missions.

QUESTION 9: If confirmed as DIRNSA, how will you ensure that U.S. Cyber Command operations and mission do not negatively impact NSA operations and mission?

If confirmed, my extensive experience in integrating operations across multiple domains will guide me in balancing the needs of both organizations. I will continuously evaluate and synchronize the efforts of both agencies. By maintaining a unity of effort and rigorously enforcing resource management processes, I will protect the NSA's core missions while effectively supporting USCYBERCOM's' objectives.

Keeping the Congressional Intelligence Committees Fully and Currently Informed

QUESTION 10: Please describe your view of the NSA's obligation to respond to requests for information from Members of Congress.

To ensure the Congressional intelligence committees have the necessary information to carry out their authorized responsibilities, it is the obligation of the Director of the NSA to keep the intelligence committees fully and currently informed of all of NSA's intelligence activities consistent with the constitutional and statutory obligations of the Executive Branch.

QUESTION 11: Does NSA have a responsibility to correct the record, if it identifies occasions where inaccurate information has been provided to the congressional intelligence committees?

Absolutely, and if confirmed, I look forward to working with the Committee to ensure transparency and the accuracy of information provided to Congress.

QUESTION 12: Please describe your view on when it is appropriate to withhold pertinent and timely information from the congressional intelligence committees.

NSA has an obligation to keep the Congressional intelligence committees fully and currently informed of all its intelligence activities. I understand there is a process for presenting highly sensitive information with select Congressional leadership instead of with an entire oversight committee. If confirmed, I will strive to accommodate Congress' need for information to perform its critical oversight function including rare circumstances such as those involving Executive Branch confidentiality interests.

National Security Threats and Challenges Facing the Intelligence Community

QUESTION 13: What, in your view, are the current principal threats to national security most relevant to the NSA?

From my perspective, the full spectrum of threats from China; increasing volatility and the risk of crisis and conflict in multiple theaters; accelerating technological change; and the targeting of U.S. critical infrastructure and U.S. political and economic targets. If confirmed, I am committed to ensuring NSA remains the world's' best SIGINT and cybersecurity agency, providing exquisite intelligence and expertise for our nation.

QUESTION 14: 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?

My understanding is NSA plays a key role in the IC in meeting the significant challenge of ubiquitous encryption. Cryptography is a foundational, core competency of NSA. I believe NSA has the skilled talent and access to additional talent, technical capabilities, and the global enterprise and is uniquely positioned to play a central role in the government's work to address this challenge, consistent with direction provided by the Department of War and the Office of the Director of National Intelligence (ODNI).

QUESTION 15: Do you believe that the IC needs additional statutory authorities to address the proliferation of ubiquitous commercial encryption?

It is my understanding that currently the IC, particularly the NSA, has legal authorities that enable it to generate valuable foreign intelligence while safeguarding the constitutional rights, civil liberties, and privacy of U.S. citizens. If confirmed, I intend to evaluate how the NSA uses these authorities and ensures compliance with privacy protections.

QUESTION 16: The priorities and objectives of DIRNSA have frequently been shaped by external events and conditions, as well as requests from the Executive Branch. What do you see as the foremost external factors shaping your priorities and objectives as DIRNSA? What do you see as the foremost expectations placed on DIRNSA by the current Executive Branch?

The principal foreign threats facing the nation include the full spectrum of threats from state and non-state actors; increasing volatility in the strategic environment; accelerating technological change; and cyber threats to U.S. national security systems, critical infrastructure, and political and economic targets. The foremost expectations NSA has from the executive branch are that the Agency is aligned with the President's priorities—articulated through the National Intelligence Priorities Framework—and delivers results as good stewards of the nation's resources, while safeguarding constitutional rights, civil liberties, and privacy of Americans.

Foreign Intelligence Surveillance Act

QUESTION 17: Title VII of the Foreign Intelligence Surveillance Act (FISA) will sunset on April 20, 2026, including what is commonly known as Section 702. Please describe the significance of Section 702 collection to NSA, the IC, and based on your previous roles, the U.S. warfighter. If Section 702 authorities were to end or be diminished, what would be the impact on national security?

Throughout my career, I have been a consumer of the intelligence collected thanks to FISA 702, which has provided critical, deep understanding of our nation's adversaries. In my experience, the intelligence provided, obtained from the communications of foreign individuals outside the United States who are reasonably believed to possess foreign intelligence information, has saved the lives of Americans and our allies and partners. It is a valuable authority that provides key insights into foreign adversaries and helps us

understand and stay ahead of foreign threats. If confirmed, I will utilize all available authorities to advance NSA's' foreign intelligence mission while protecting Americans' privacy and civil liberties, and I am fully committed to working with Congress on matters related to this authority.

QUESTION 18: Do you support the reauthorization of Section 702?

As a current customer of FISA Section 702-derived intelligence products, I recognize this authority provides key insight into foreign adversaries and helps us understand and stay ahead of foreign threats. It is crucial to protecting the nation from current and emerging threats by providing critical insights into our most challenging adversaries. I also swore an oath to support and defend the Constitution, which includes protecting American civil liberties, so I recognize the importance of ensuring that those who operate within the authorities of Section 702 comply with oversight requirements. If confirmed, I commit to working with Congress on matters related to this authority.

QUESTION 19: What amendments, if any, to Section 702 or other provisions of FISA do you believe are necessary?

Due to the time constraints of the reauthorization of FISA Section 702, if confirmed, this will be a top priority, and I will quickly assess whether to recommend any amendments or provisions to the Administration. I will provide my best military advice to the Administration and Congress on matters related to this authority.

QUESTION 20: Please describe why it is necessary for the NSA to have the ability to perform U.S. person queries of information acquired pursuant to Section 702 of FISA. What are the implications of requiring NSA to seek a court order based on probable cause prior to performing such queries, and how would this affect national security?

At this time, I defer to NSA leadership to characterize the existing efforts taking place under this authority. If confirmed, I fully commit to working with Congress on matters related to this authority.

QUESTION 21: Please describe the compliance regime that the NSA has in place for its Section 702 collection authorities.

It is my understanding that NSA has invested immense effort and resources to ensure the compliance process is robust and thorough, reflecting an unwavering commitment to protecting Americans' privacy and civil liberties. If confirmed, I fully commit to working with Congress on matters related to this authority.

Cybersecurity and Artificial Intelligence

QUESTION 22: What role do you see for the NSA in defensive cybersecurity policies or actions? What role do you see for the NSA in supporting any U.S. Government offensive cybersecurity policies or actions?

As the National Manager for National Security Systems, it is my understanding that NSA is the U.S. Government focal point for cryptography, and information systems security for National Security Systems. In this role, NSA prevents and eradicates threats to these systems, including by examining U.S. Government national security systems and evaluating their vulnerability to foreign interception and exploitation. NSA also provides critical threat intelligence on foreign cyber threats to those national security systems. Similarly, I understand NSA, as a combat support agency, is a critical supplier of SIGINT to support the warfighter and enable the Department of War to maintain enduring advantages over our adversaries in cyberspace.

QUESTION 23: What should be the NSA's role in helping to protect U.S. commercial computer networks that are not part of the defense industrial base?

Multiple federal departments and agencies, including NSA, play a role in helping to protect the U.S., including the commercial sector, from cyber threats. The complex and interconnected threat environment requires a multi-faceted approach. I understand that NSA has close relationships across the federal government and the private sector, and if confirmed, I intend to continue building and strengthening these relationships.

Within NSA, I understand that an entire directorate implements the Agency's cybersecurity responsibilities to ensure NSA is postured to contribute to the protection of National Security Systems, the Department, and the DIB. I also understand that NSA has developed significant relationships with the DIB and its service providers to share threat information and provide cybersecurity support. The support to service providers, such as cybersecurity and internet service providers, also helps to scale protection across the United States. The

Artificial Intelligence (AI) Security Center within this directorate fuses NSA's expertise in AI research, cybersecurity, and foreign intelligence to detect and mitigate malicious cyber threats to AI systems within the Department, to National Security Systems, and the DIB, which includes partnering with private industry and publishing guidance to prevent or mitigate counter AI techniques. If confirmed, I am committed to continuing to enhance NSA's efforts.

QUESTION 24: 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?

Though private-sector entities have the primary responsibility for the security of their systems, I believe the U.S. government has a responsibility to share specific threat information to those networks with private sector entities whenever possible, consistent with NSA's authorities. I understand NSA has made significant progress in scaling its sharing of foreign cyber threat information with the DIB and its service providers, as well as with AI companies to ensure they have the information they can use to protect their networks. If confirmed as Director, I will ensure NSA continues to engage with these companies to share unclassified information that is helpful and enables the entities to appropriately protect their networks while still ensuring the necessary protection of classified threat information.

QUESTION 25: Should NSA publish finished cybersecurity intelligence products? Why or why not?

As a consumer of NSA's intelligence products in my current role as Deputy Commander USINDOPACOM, I recognize the value of NSA's intelligence products and I can state, without reservation, that the nation is well served by the dedicated work conducted by NSA's analytic workforce. If confirmed, I will review current NSA intelligence product types and make an assessment based on mission requirements and resources whether existing products meet customer needs.

QUESTION 26: What are your views on artificial intelligence (AI) and the roles that it can play in cybersecurity and intelligence? If confirmed, how do you intend to invest in this technology?

My understanding is that NSA has been at the forefront of AI innovation for over six decades, evolving from early applications in pattern recognition for encrypted data to today's sophisticated AI systems that defend against nation-state cyber threats. As we enter a new era of strategic competition, our ability to effectively leverage AI has become crucial to maintaining our technological edge over adversaries.

AI as a cutting-edge technology is absolutely something I would expect NSA and USCYBERCOM to continue to develop if I am confirmed. AI represents a transformative capability that fundamentally enhances NSA's ability to fulfill its critical national security mission. As the volume, velocity, and complexity of data continues to grow exponentially, AI enables NSA to process and analyze information at unprecedented speed and scale, uncovering threats and insights that would be impossible to detect through human analysis alone.

Addressing evolving cybersecurity threats requires a multi-faceted approach. AI can enhance NSA's cybersecurity measures by identifying vulnerabilities and responding to threats in real time.

NSA Capabilities

QUESTION 27: What are your views concerning the quality of NSA's intelligence collection, and what is your assessment of the steps that the NSA has taken to date to improve that collection?

As an intelligence customer, I have found that NSA's reporting provides deep, unique insights into adversary activities. From my post in USINDOPACOM, I have not received information on efforts to improve NSA's collection capabilities. If confirmed, I will identify and address areas in which NSA collection capabilities can be improved or changed.

QUESTION 28: If confirmed, what additional steps would you pursue to improve intelligence collection and what benchmarks will you use to judge the success of the NSA's future collection?

Based on my experiences, a key benchmark for the efficacy of NSA collection should be intelligence customer feedback. Under my leadership, I pledge to assess how NSA's collection posture can be optimized to deliver timely and accurate intelligence to decision makers and warfighters.

QUESTION 29: What is your assessment of the quality of current NSA intelligence analysis?

In my role at USINDOPACOM, I have benefited greatly from NSA's intelligence products and believe the nation is well served by the work of NSA's dedicated analytic workforce. I understand NSA's reporting is the result of robust training, tradecraft, and subject-matter expertise. If confirmed, I plan to continue NSA's investment in its analytic personnel and ensure those resources are aligned with the National Security Strategy.

QUESTION 30: 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?

If confirmed, I intend to continue NSA's prioritization of hiring, training, and maintaining the Agency's extraordinarily talented workforce, which I believe is key to NSA's analytic production. I will also ensure NSA is making the investments necessary for the tools to maintain its technological edge in its analytic production, particularly in the field of AI. I understand NSA uses several technical tools to assess the value of its intelligence production, and if confirmed, I will instruct my leadership team to use these qualitative and quantitative assessment tools to inform leadership decision-making and ensure NSA's analytic efforts are properly aligned to current priorities. I will also commit to engaging with customers in the IC, military, and decision makers to receive direct feedback.

QUESTION 31: 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 the NSA should produce.

At USINDOPACOM, we rely heavily on the NSA's strategic analysis to understand the intentions and capabilities of our adversaries, to anticipate future challenges, and to develop and refine our theater strategy. While my focus has been on the operational application of this analysis, I have a deep appreciation for its foundational importance. Strategic analysis provides the "so what" that enables us to move from simply knowing what is happening to understanding what it means for our national security interests. If confirmed, I would be dedicated to ensuring that the NSA produces the world-class strategic analysis that our nation's leaders, and our warfighters, depend on.

QUESTION 32: What are your views on the role of foundational research to the NSA's mission?

Foundational research plays a critical role in advancing the NSA's emerging capabilities, as it underpins the agency's ability to address rapidly evolving threats, maintain superiority, and safeguard national security. Foundational research postures NSA to plan for the technology of tomorrow and out-maneuver our adversaries, who are highly capable of using and exploiting advanced technologies to compete with us and do us harm.

The NSA operates in a rapidly changing technological environment, where adversaries continuously develop new capabilities at very low cost in areas such as cyberwarfare, AI, and information warfare. Foundational research ensures the NSA remains at the forefront of innovation, enabling it to anticipate and effectively counter emerging threats with partnership across the IC and the Department.

NSA Personnel

QUESTION 33: 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?

I look forward to learning more about the unique parameters that guide the use of contractors at NSA. In my experience at USINDOPACOM and in U.S. Special Operations, the use of contractors to fulfill intelligence-related functions should be guided by principles that ensure mission effectiveness, fiscal responsibility, and adherence to security and ethical standards.

If confirmed, it is my intent to learn more about each of the following principles:

1. **Accountability and Oversight**. Learn about the oversight mechanisms to ensure contractors perform their duties in full compliance of all laws, ethically, and in alignment with the agency's mission and values. Contractors must meet the same rigorous security clearance and

compliance standards as government employees to protect classified information and ensure the integrity of intelligence operations.

2. **Speed and Scalability**. If confirmed, I intend to learn more about the opportunities that contractors can provide for capability acceleration and increased capacity. These are critical to remain ahead of emerging threats and technological advancements.

3. **Mission Alignment**. Contractors should be utilized for tasks that require specialized expertise, surge capacity, or short-term support, while inherently governmental functions—such as decision-making, oversight, fiscal or resource management, and activities involving sensitive intelligence sources and methods—should remain the responsibility of full-time government employees.

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

In my experience, various elements within the DoW and IC have effectively used contractors in support roles to accomplish their missions. Drawing from my past and present military leadership experiences, I would surmise that suitable contractor support functions might include professional services, engineering and technical assistance, IT services, and facilities operations and maintenance services.

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?

Yes. Inherently governmental functions should not be conducted by contractors. Inherently governmental functions are those functions that possess a significant and intimate relation to the public interest and therefore require performance by federal government employees to ensure appropriate accountability.

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

From my perspective, any government agency or organization should carefully weigh the costs of contractors against those of government employees. I believe it is essential to maintain a balanced workforce composition of both government and contractor personnel. If confirmed, I plan to familiarize myself with the specific costs and benefits of each and leverage my experience from lean and specialized special operations organizations, that continuously evaluated organization design for a strategic workforce complement, that leverages the surge and technical advantages of contractors, and the deep enduring knowledge of government civilian talent. If confirmed, I will thoughtfully consider this issue to help the agency achieve the optimal workforce balance.

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

The NSA must have leaders who fully understand the agency's operational needs and mission requirements and have up-to-date and precise data on the workforce composition. It is important to assess mission requirements, identify which functions are inherently governmental, and determine the appropriate manpower mix to maintain mission capability. If confirmed, I plan to delve deeper into this area to assess if any specific enhancements, policies, or tools are needed to ensure the right mix of government civilians, military personnel, and contractors within the NSA's workforce.

QUESTION 34: What is your assessment of the NSA’s current personnel accountability system?

From my current position at USINDOPACOM, I do not have insight into NSA’s current personnel accountability system. If confirmed, I commit to understanding this system and addressing areas that require improvement.

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?

In my current role at USINDOPACOM, I have limited insight in the IC process for handling personnel accountability. If confirmed, I commit to conducting further analysis on existing NSA processes and ensure that any personnel accountability system is equitable and has appropriate due-process protections.

Security Clearance Reform

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

A strong, rigorous, and fair clearance process is central to NSA's ability to hire and retain a talented and trusted work force. A robust clearance process is the Agency's first line of defense against insider threats and those who wish to do harm to the nation. If confirmed, I commit to ensuring that NSA's security clearance processes are fully in line with applicable law and policies.

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

If confirmed, I commit to ensuring that NSA' security-clearance processes are fully in line with applicable law and policies. I look forward to working with community stakeholders to identify and implement additional efficiencies and improvements in NSA's process as appropriate.

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?

The NSA has a long history of producing timely, actionable and non-partisan SIGINT in compliance with governing legal authorities and analytic integrity standards. If confirmed, I will reinforce this core standard—making clear to NSA's analysts that their guiding principle is independent intelligence analysis, regardless of their target or customer.

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

If confirmed, I commit to ensuring that NSA’s intelligence products adhere to NSA and IC Analytic Integrity Standards by validating that Agency personnel receive appropriate training and oversight. Under my leadership, the importance of analytic objectivity and integrity being built into NSA’s overall culture of compliance.

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?

I have always provided accurate and factual assessments to policymakers. If confirmed, I will continue this commitment of speaking truth to power and ensuring our policymakers have accurate information to inform their decision-making process.

QUESTION 39: What are your views of the current NSA culture and workforce?

In my interactions with NSA, I have always been struck by their strong emphasis on dedication to the mission, technological innovation, professionalism, and a commitment to legal compliance and privacy protections. The workforce is highly skilled. If confirmed, I look forward to gaining a deeper understanding of the agency's culture and workforce dynamics to ensure that the NSA continues to operate effectively and in accordance with the law to support the American warfighter and policymakers, while always looking for ways to enhance speed, agility and scale.

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

If confirmed, I intend to foster a culture that is dedicated to answering our policymaker's toughest questions and providing support for our warfighters' most pressing intelligence and cybersecurity needs. I am a leader that is in a relentless pursuit of excellence, through meaningful challenges that offer satisfaction when addressed. I will permeate this culture across the civilian, military and contractor workforce at NSA, to include the field sites. This culture will be infused with deep commitments to compliance with law and policies and protections of Americans' civil liberties and privacy.

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

If confirmed, ensuring that the dedicated professionals at NSA feel supported and valued is essential for maintaining the agency's effectiveness and its critical role in national security. One of my priorities will be to engage with the NSA workforce to gain a deeper understanding of their challenges and to work with the NSA leadership team to address any concerns, including issues related to morale.

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

Throughout my career, I have learned the enduring advantage in any organization is the workforce. If confirmed, I plan to encourage collaboration, maintain open communication channels to address concerns, and ensure the collective workforce is dedicated to NSA's shared mission. If confirmed, I look forward to assessing the current relationship between the civilian and military members of the NSA workforce and implementing any changes necessary to accomplish the mission.

Transparency

QUESTION 40: Do you believe that intelligence agencies need some level of transparency to ensure long-term public support for their activities?

Transparency is a pillar of maintaining trust. While the sensitive nature of the intelligence agencies' work requires a high degree of secrecy, the agencies must strive to share as much information as possible about their mission, authorities, and oversight mechanisms without compromising sources and methods. Building public trust through appropriate transparency is vital for maintaining support for our critical national security missions. If confirmed, I commit to working with the Department and policymakers to build public trust in a manner consistent with the constitutional and statutory obligations of the Executive Branch.

QUESTION 41: If confirmed, what would be your approach to transparency?

It is essential that NSA be accountable to entities who have oversight authorities and to the American public, and some level of transparency is essential to ensuring accountability. If confirmed, I will work to prevent foreign adversaries from learning our secrets and capabilities while providing transparency on our activities through appropriate mechanisms, to include engagements with this Committee.

Disclosures of Classified Information

QUESTION 42: In your view, does the NSA take appropriate precautions to protect classified information and prevent, deter, investigate, and punish unauthorized disclosures of classified information?

Everything in my past experience indicates this is absolutely the case. Intelligence Community professionals are entrusted with highly sensitive information, and with that trust comes profound responsibility. If confirmed, protecting NSA information will be a top priority, and I will use my authorities and influence to deter and investigate instances of misuse of classified information. Those who misuse classified information to harm our mission or nation should be punished to the fullest extent of the law.

QUESTION 43: If confirmed, how will you ensure that appropriate and necessary precautions to protect classified information are maintained and improved, if necessary?

We cannot afford to allow malign actors to jeopardize the vital work of NSA and the security of our nation. If confirmed, I commit to making sure NSA has the right personnel—dedicated security and counterintelligence professionals who educate the workforce and investigate and prevent unauthorized disclosures—and the right technology, to ensure classified information is controlled and protected.

QUESTION 44: If confirmed, how would you manage 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.

Each of these issues is tied to NSA's core requirements for enterprise resilience and protection. If confirmed, I plan to take an all-encompassing look at NSA systems, recruiting, retention, talent development and security to identify any possible areas for improvement. I will ensure effective and regular

oversight of existing alignment programs such as those that "red team" to identify vulnerabilities, and those that "blue team" to develop protections. NSA's mission requires constant vigilance and continuous improvements to ensure that the Agency continues to deliver critical intelligence to its customers and protect its sources and methods.

QUESTION 45: How do you think that individuals who mishandle, intentionally or unintentionally, classified information should be dealt with?

Mishandling classified information is an extremely serious offense. Depending upon the classification of the material, the intent of the individual, and the circumstances of the case, there are a number of potential forums for corrective action—including workplace discipline, termination and revocation of a security clearance, and, when necessary, criminal penalties.

Questions from Senator Warner

QUESTION 46: In Fiscal Year 2025, Congress statutorily authorized the National Security Agency's Artificial Intelligence Security Center, with responsibilities (as amended the Intelligence Authorization Act of FY 2026) of developing guidance to address security threats to AI systems, promulgating security guidance to defense AI technologies from theft by nation-state adversaries, promoting secure AI adoption practices across the NSS, and additional functions DIRNSA considers appropriate.

a. Given the aggressive timeline for adoption of AI solutions directed by the Secretary of Defense, how will you ensure prioritized development and adoption of secure AI usage practices across the NSS?

If confirmed, I will embrace and accelerate adoption and development of AI solutions guided by Executive Order 14179, and the Secretary's Department of War AI Strategy 2026. This direct acceleration of AI adoption highlights the urgency of integrating secure and reliable AI solutions into all military operations. To ensure prioritized development and adoption of secure AI practices, I will focus on three key areas: governance, infrastructure, and workforce readiness.

First, I would establish clear governance frameworks to ensure that AI systems are developed and deployed with robust security measures, including

encryption, access controls, and continuous monitoring to mitigate risks of adversarial exploitation.

Second, I would prioritize investments in AI infrastructure, including secure datacenters and edge computing capabilities. Leveraging partnerships with private-sector leaders in AI innovation, I would ensure the latest AI models are rapidly integrated and updated across all echelons, maintaining parity with commercial advancements while adhering to security standards.

Third, I would also focus on workforce readiness by accelerating the recruitment and training of technical talent in AI roles. This includes using special hiring authorities and talent development programs to attract top-tier expertise while fostering a culture of AI use across the National Security Systems.

b. As Chief of Staff for the United States Indo-Pacific Command, what specific measures have you directed or implemented to promote secure AI adoption?

As the Chief of Staff at USINDOPACOM, I implemented and oversaw the AI adoption both at the headquarters and at the warfighter edge across the Pacific theater. I ensured that our lead elements, the J6 Directorate, J8 Directorate and the Chief Data Office, aligned AI capabilities for agile experimentation in secure and compliant manner against the priority gaps.

The diversity of implementation from solutions like autonomous systems, unmanned sensors, weapon systems and other forward tactical and operation capabilities adhered to echelon appropriate security and governance. Whereas enterprise network capabilities adhered to the appropriate military Service, DISA and Cyber Command security requirements.

c. Please provide examples of how you have overseen responsible, secure, and reliable AI adoption in your current role.

As Deputy Commander and Chief of Staff for USINDOPACOM, I have directed and implemented specific measures to promote secure and trusted AI adoption, recognizing that effective AI solutions are critical to enhancing operational efficacy, workforce efficiency, and agile technological advancement. During my tenure, we have rapidly integrated diverse machine

learning technologies, embracing experimentation, learning from failures, and adapting swiftly to develop improved use cases and capabilities. These efforts have focused on leveraging AI to enhance the "data-to-decision" process, ensuring faster, more informed decision-making that keeps pace with the dynamic information environment, near-peer threats, and the accelerating evolution of technology.

Specifically, USINDOPACOM has used AI to improve the execution of Joint Warfighting Functions as well as workflow speed. These applications have enabled the command to maintain decision advantage in a complex and rapidly changing operational landscape. To ensure secure adoption, we prioritize integrating AI solutions that are trusted, validated, and aligned with mission requirements, while adhering to ethical and legal standards.

In addition to technological integration, we have invested heavily in workforce development programs to build the skills necessary for secure and effective AI adoption. These initiatives include internal data literacy programs covering data sciences, prompt engineering, and tool-specific competencies. Equally important, we have focused on developing leaders who consume information for decision-making from authoritative and validated data sources, supported by visualizations that leverage automation and agentic machine learning capabilities. By fostering a culture of trust, innovation, and continuous learning, we have ensured that AI adoption is not only secure but also embraced as a transformative enabler for USINDOPACOM's mission success.

d. Are there additional functions for the AI Security Center that you contemplate?

If confirmed, I intend to prioritize a comprehensive and in-depth understanding of the functions and operations of the AI Security Center. I recognize the Center excels in leveraging foreign intelligence insights to fortify the security and resilience of U.S. AI systems, ensuring they remain impervious to adversarial exploitation.

In pursuit of this, I anticipate a significant and impactful outcome will be the strategic prioritization of capabilities that must be safeguarded to optimize national defense, enhance the warfighter's operational advantage, and bolster strategic deterrence. By identifying and protecting these critical

capabilities, we can ensure AI technologies are not only secure but also serve as transformative enablers for the defense of the homeland and the advancement of U.S. national security objectives.

QUESTION 47: National Security Memorandum 8 (NSM-8) provides DIRNSA, in their role as National Manager for National Security Systems (NSS), with the authority to issue Binding Operational Directives and Emergency Directives to safeguard NSS. In discharging this responsibility, DIRNSA may encounter circumstances in which elements of the Department of Defense, including combatant commands, have failed to adopt adequate security measures, often citing mission priorities. As DIRNSA, will you ensure that the security, resilience, and integrity of overall NSS take priority, including when in tension with more narrow mission objectives?

Yes.

a. Are there examples in your present command in which you have failed to timely implement a Binding Operational Directive or Emergency Directive? If so, please provide the Committee with a detailed description of the rationale for untimely implementation.

USINDOPACOM has complied with all Binding Operational Directives (BODs) and Emergency Directives (EDs) to the maximum possible extent that also meets critical mission objectives or has sought an exception to policy (ETP) or timeline extension (via an approved Project Objectives and Milestones (POAM)) where additional resources (time, personnel, money, technical solution, or other) are required to achieve compliance.

c. Are there examples in your present command in which you have sought exceptions from a Binding Operational Directive or Emergency Directive? If so, please provide the Committee with a detailed description of the rationale for each exception sought.

USINDOPACOM has submitted and received the requisite ETPs or timeline extensions (via a POAM) to meet all BODs and EDs. USINDOPACOM-assigned Service Components are responsible for service-related networks/systems requirements. The USINDOPACOM J6 Director is

responsible for the preponderance of the theater Mission Partner Environment (MPE), with the exception of select niche capabilities that are service-peculiar.

Questions from Senator Wyden

Definition of Signals Intelligence

QUESTION 48: During his confirmation process, former director Haugh wrote that:

"The definition of signals intelligence applicable to NSA is found in DoDM S5240.01-A (the SIGINT Annex) that, at Section 1.2, defines SIGINT to include, individually or in combination, communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT)."

The DIRNSA serves as the Intelligence Community's Functional Manager for SIGINT. As the nominee for that position, do you see that definition as applying to other elements of the IC? If not, how do different elements define SIGINT differently?

In my current role with USINDOPACOM, I am not aware of any misalignment across IC elements on this matter. I understand that NSA's activities under Executive Order 12333 are governed by Attorney General-approved guidelines, which contains the definition referenced above. This definition matches a jointly developed definition of SIGINT coordinated by the Office of the Director of National Intelligence in response Sec. 309(a) of the FY 2022 Consolidated Appropriations Act, Division X. If confirmed, I look forward to studying this issue further and engaging with the Committee as necessary.

FISA Section 702

QUESTION 49: During her confirmation process, Director Gabbard wrote: "Warrants should generally be required before an agency undertakes a U.S. Person query of FISA Section 702 data, except in exigent circumstances, such as imminent threats to life or national security." During his confirmation process, Principal Deputy Director Lukas agreed. Do you also agree?

As a current customer of FISA Section 702-derived intelligence products, I recognize this authority provides key insight into foreign adversaries and helps us understand and stay ahead of foreign threats. At this time, I defer to NSA leadership to characterize the existing efforts taking place under this authority. If confirmed, I fully commit to working with Congress on matters related to this authority.

QUESTION 50:

During his confirmation process, now former Assistant Attorney General for National Security John Demers was asked about the prohibition on reverse targeting in Section 702 of the Foreign Intelligence Surveillance Act (FISA). He responded:

"As I understand it, determining whether a particular known U.S. person has been reverse targeted through the targeting of a Section 702 target necessitates a fact specific inquiry that would involve consideration of a variety of factors. For example, as the Privacy and Civil Liberties Oversight Board noted in its 2014 report, if a Section 702 tasking resulted in substantial reporting by the Intelligence Community regarding a U.S. person, but little reporting about the Section 702 target, that might be an indication that reverse targeting may have occurred."

During his confirmation process, former Director Haugh wrote that: My understanding of whether reverse targeting has occurred comports with that of Mr. Demers…" During his confirmation process, Principal Deputy DNI Lukas wrote that "My understanding is that, consistent with Assistant Attorney General Demers' statement, IC elements make fact-specific determinations and consider a variety of factors to ensure that Section 702 is not used for reverse-targeting of U.S. Persons." Do you also agree with the process outlined by Mr. Demers?

I understand that reverse targeting is prohibited under FISA Section 702. However, in my current role at USINDOPACOM, I am not involved in the oversight of NSA's use of FISA Section 702, and I do not have insight into the current processes surrounding the investigation, substantiation, and mitigation of FISA compliance incidents. At this time, I defer to NSA leadership to fully characterize the existing efforts taking place under this authority. If confirmed, I fully commit to working with Congress on matters related to this authority.

Encryption

QUESTION 51: During her confirmation process, Director Gabbard wrote that: "Mandating [to the manufacturers of electronic devices or software for electronic devices] mechanisms to bypass encryption or privacy technologies undermines user security, privacy, and trust, and poses significant risks of exploitation by malicious actors." Do you agree?

Encryption is essential to NSA's cybersecurity activities that include the protection of critical National Security Systems. I am committed to ensuring we have the tools we need to protect the nation while upholding the fundamental security and privacy that all Americans expect. If confirmed, I look forward to studying this issue further and commit to further engagement with the Committee on this topic and other important matters.

Transparency

QUESTION 52: Will you support the declassification and public release of any interpretation of law that provides a basis for intelligence activities, but is inconsistent with the public's understanding of the law?

Intelligence agencies must exercise a level of transparency that showcases trust, transparency and fosters long-term public support for their activities. While the sensitive nature of the intelligence agencies' work requires a high degree of secrecy, the agencies must strive to share as much information as possible about their mission, authorities, and oversight mechanisms without compromising sources and methods. If confirmed, I commit to working with the Administration and Congress to build public trust in a manner consistent with the constitutional and statutory obligations of the Executive Branch.

Competitive Advantage

QUESTION 53: Executive Order 14086, Enhancing Safeguards for United States Signals Intelligence Activities, states: "It is not a legitimate objective to collect foreign private commercial information or trade secrets to afford a competitive advantage to United States companies and United States business sectors commercially."

a. How will you ensure that NSA does not violate this prohibition?

b. If asked to collect intelligence in violation of this prohibition, will you promptly notify the Committee?

If confirmed, I will ensure NSA conducts its SIGINT mission in accordance with governing legal authorities and commit to keeping the Intelligence Committees fully and currently informed of all of NSA's intelligence activities consistent with the constitutional and statutory obligations of the Executive Branch. At this time, I defer to NSA leadership to fully characterize the existing efforts taking place under this authority.

Personnel Policies

QUESTION 54: 10 USC §1609 grants the Secretary of Defense the authority to terminate the employment of an employee in a defense intelligence position if the Secretary considers the termination to be in the interests of the United States and determines that the procedures prescribed in other provisions of law that govern terminations cannot be invoked in a manner consistent with the national security. 10 U.S.C. §1609(c) requires that any such termination shall be promptly notified to the congressional oversight committees.

a. Will you ensure that any use of Section 1609 to terminate an employee of the NSA is promptly notified to the congressional intelligence committees?

If confirmed I will work with the Secretary to ensure all actions and notifications adhere to applicable laws.

b. Will you ensure that such notifications include an explanation for why the termination is determined to be in the interest of the United States and why termination procedures cannot be invoked in a manner consistent with the national security?

If confirmed, I look forward to studying this issue further and commit to further engagement with the Committee and the Secretary on this and other important matters.

SELECT COMMITTEE ON

INTELLIGENCE

UNITED STATES SENATE

Post-Hearing Questions for the Record for

Lt. Gen. Joshua M. Rudd

upon his nomination to be

Director of the National Security Agency

From the Vice Chairman

Election Security

1. What is your understanding of the scope of NSA's authorities with respect to election security? What are the limits on NSA's ability to engage in domestic activities related to election security?

I understand that NSA has provided critical foreign intelligence insights into foreign actors that aim to influence and/or interfere with our elections. Other interagency partners have the primary responsibility for domestic activities in relation to election security.

From Senator Collins

Cyber Command Prevention of Breaches

2. How do you intend to ensure Cyber Command isn't just reacting to breaches, but proactively preventing them?

We proactively control the battlespace in all warfighting domains through deliberate planning activities and campaigning to ensure advantage for friendly forces. In cyberspace, USCYBERCOM is already leveraging information at machine speed; harnessing automation for widespread repetitive tasks; and integrating artificial intelligence/machine learning (AI/ML) wherever possible—not only to prevent breaches but also to predict and shape the operational environment. If confirmed for this role, I intend to accelerate those efforts at every opportunity to protect our networks and assets.

Integration with State, Local, and Private Sector Partners

3. When it comes to critical domestic vulnerabilities such as terrorist and cybersecurity threats, the source of intelligence often comes from one of the two commands which you are nominated to lead today. State and local governments, businesses, and critical infrastructure sites need to have a trusted Federal element to go to for quick support before a cyber or terrorist attack occurs. As the nominee to direct the largest cyber and communications agency in the Federal government, how do we get timely and critical information to those who need to heed these warnings?

The cyber landscape is constantly evolving, with a growing reliance on emerging technologies such as AI, expanding attack surfaces and an ever-increasing interconnection of devices across sectors. If confirmed, I will continue to focus on the foreign intelligence advantage our signals intelligence (SIGINT) capabilities bring to understand the threats against the homeland. While NSA remains focused on securing U.S. national security

systems (NSS), the Defense Industrial Base (DIB), and the technology and cybersecurity companies capable of defending the DIB and NSS, it will continue to be imperative to share timely, actionable and relevant intelligence through our interagency partners to critical infrastructure owners and operators across all sectors. When we work across the government and with industry, we proactively harden core technologies we all rely upon and disrupt adversary campaigns at scale. If confirmed, I will continue to expand upon this industry and interagency collaboration model, to build and maintain the strong relationships required to quickly get intelligence into the hands of those who need it.

NSA Collection Against Threat Actors

4. Russia, Iran, North Korea and China are likely to continue to take up the preponderance of your command's efforts. However, I remain concerned about the growing threat of terrorism from Al Qaida and ISIS, across regions such as the Middle East, and central Africa. Terrorist attacks are occurring today in Nigeria, Syria, Iraq, Somalia, and Pakistan. However, the greatest threat to U.S. citizens overseas and within our own country remains terrorists who intend to do us harm today. Do you believe the NSA is sufficiently postured to balance collection against terrorists and other threat nations?

As all who have served our nation since 9/11 know, the counterterrorism fight requires constant vigilance to ensure the safety of the American people. Core to NSA's foreign intelligence mission is the responsibility to detect and understand foreign terrorist threats to the homeland. If confirmed, I commit to ensuring that the critical counterterrorism (CT) mission is postured to provide timely and accurate CT threat intelligence to the interagency, to help prevent and deter terrorist actions wherever American interests are present, while making sure we are also positioned to address a multitude of other national security threats. Innovation and continued integration of cutting-edge technology will serve as a force multiplier to help ensure we are postured to address multiple, complex threats simultaneously.

From Senator Wyden

Intelligence Collection Legal Safeguards

5. The NSA is bound by non-statutory rules, guardrails and procedures, to include Executive Order 12333, Executive Order 14086 ("Enhancing Safeguards for United States Signals Intelligence Activities"), Presidential Policy Directive 28 ("Signals Intelligence Activities"), DoD Manual S-5240.01-A ("Procedures Governing the Conduct of DoD Intelligence Activities; Annex Governing Signals Intelligence Information and Data Collected Pursuant to Section 1.7(c) of E.O. 12333"), and "Procedures for the Availability or Dissemination of Raw Signals Intelligence

Information by the National Security Agency Under Section 2.3 of Executive Order 12333 (Raw SIGINT Availability Procedures)." All of these documents are public.

a. If NSA is directed to operate in contravention of these public documents, will you commit to informing the public?

b. If the administration withdraws or modifies any provisions of these public documents, will you ensure that the modified documents are immediately made public?

[Response to 5a and b] Transparency is key to maintaining public trust. This must be balanced with the sensitive nature of the intelligence agencies' work, which requires a degree of secrecy to ensure we do not compromise the sources and methods that enable crucial intelligence for our warfighters and policymakers. If confirmed, I commit to working with the Administration and with Congress to share as much information as possible with the public about NSA's mission, authorities, and oversight mechanisms without compromising those sources and methods that help keep our nation safe.

Purchase of Commercially Available Data

6. In December 2023, then-Director Nakasone informed me that "NSA does not buy and use location data collected from phones known to be used in the United States either with or without a court order." Director Nakasone added, "Similarly, NSA does not buy and use location data collected from automobile telematics systems from vehicles known to be located in the United States."

a. Will you ensure that NSA does not purchase, or otherwise obtain these forms of location data?

b. Since Director Nakasone's assurances were unclassified, will you ensure that the public is informed of any deviations from that policy?

[Response to 6a and b] This is an issue I would like to understand better given my limited familiarity in my current role at USINDOPACOM. If confirmed, I commit to studying this issue more closely.

7. Then-Director Nakasone's December 2023 letter stated: "NSA does buy and use commercially available netflow (i.e. non-content) data related to wholly domestic internet communications and internet communications where one side of the communication is a U.S. Internet Protocol address and the other is located abroad." What commercially available netflow data do you believe is appropriate for NSA to purchase? Does it include internet browsing records of persons in the United States? Please respond with regard to wholly domestic internet communications and communications where one side is located abroad.

I understand that NSA has two separate, but closely related missions: the collection and analysis of foreign SIGINT, and the protection of U.S. national security systems, the Department, and the DIB. NSA implements its cybersecurity mission by partnering with other U.S. Government agencies, allies, industry, academia, and researchers. As our foreign cyber adversaries do not stop at the U.S. border, these partnerships are key to fully understanding and helping to prevent foreign cyber threats targeting critical U.S. systems. I believe it is vital that in performing these missions, we find the right balance between Americans' civil liberties and privacy and cybersecurity.

I have limited familiarity with this specific issue in my current role at USINDOPACOM. If confirmed, I will study this issue further.

From Senator Ossoff

Intelligence Collection Legal Safeguards

8. Many of NSA's intelligence collection activities are not regulated by the Foreign Intelligence Surveillance Act (FISA) or other statutes, but are instead governed by regulations established pursuant presidential directive, including procedures issued pursuant to Executive Order 12333. For example, the so-called "SIGINT Annex" (DoD Manual S-5240.01-A) sets forth the primary procedures governing the collection, processing, and dissemination of most forms of SIGINT not otherwise subject to FISA, including limitations on collection targeting U.S persons or persons inside the United States. Unlike statutes, presidential directives can be waived by the President.

a. If the President waives a requirement set forth in Executive Order 12333, or procedures issued pursuant to Executive Order 12333, and orders the NSA to engage in an activity that would have been prohibited but for that waiver, will you commit to immediately notifying the congressional intelligence committees consistent with the statutory requirement to keep the committees fully informed?

If confirmed, I commit to keeping the intelligence committees fully and currently informed of the Agency's intelligence activities, consistent with the Constitutional and statutory obligations of the Executive Branch.

From Senator Bennet

General

You are nominated to lead a military intelligence agency with extraordinary surveillance capabilities – and this Committee is considering your nomination at a time when many Americans are following events in Minneapolis with great concern.

One of the revelations from the Church and Pike Commissions was the improper surveillance of protesters. Senator Frank Church later warned of the possibility that

the National Security Agency's (NSA) incredible surveillance capabilities "could be turned around on the American people." Specifically, he said that "the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know."

This Committee's charge is to ensure that the NSA operates within the law and under proper supervision – so that we never cross into what Senator Church referred to as the "abyss" of "total tyranny."

9. Do you commit to act consistent with the Constitution and to ensure that the National Security Agency will not use its authorities to gather intelligence on ordinary Americans exercising their constitutional rights to protest any presidential Administration's actions and policies?

The protection of the American people, our values, and our homeland are the principles that have underpinned my entire military career. If confirmed, these same principles will guide my leadership of the NSA. I commit to ensuring that NSA—guided by the protection of American civil liberties and privacy—will conduct its foreign intelligence mission in accordance with the Constitution and with all applicable laws.

10. Do you agree that military intelligence agencies, including the NSA, should be focused on gathering insights into our foreign adversaries, not insights into any American president's domestic political opponents?

NSA fosters a robust culture of providing accurate, timely, and non-partisan foreign intelligence to policymakers and warfighters that I will continue, if confirmed. I will ensure that NSA conducts its foreign intelligence mission in accordance with the Constitution and all governing legal authorities.

According to publicly available information, NSA Colorado (NSAC) works alongside the National Reconnaissance Office and the National Geospatial-Intelligence Agency-Denver to produce integrated intelligence to defense, intelligence, and civil agencies supporting the U.S. government and its allies. NSAC is the overhead technical SIGINT collection and processing enterprise center, the global overhead SIGINT mission management hub, a cryptologic discovery leader, and the electronic intelligence (ELINT) analysis and tradecraft development focal point for the NSA/Central Security Service enterprise.

11. Do you commit to work with the Committee to sustain and support NSAC's important contribution to U.S. national security, including in these areas?

If confirmed, I commit to working with the Committee to sustain and support the critical missions being undertaken at NSA Colorado.

Foreign Intelligence Surveillance Act

Many Members on this Committee appreciate that the Foreign Intelligence Surveillance Act (FISA) is a critical intelligence collection tool that helps to protect our national security. When Section 702 was last reauthorized by Congress in 2024, we enhanced protections for privacy and civil liberties. As we contemplate the renewal of Section 702, we will be assessing the efficacy of those protections and checking to ensure that there have been no abuses.

12. Do you commit to ensure that the NSA will not turn corners and will abide by the law when exercising its authorities to collect intelligence pursuant to FISA, including Section 702?

If confirmed, I commit to ensuring that NSA, guided by the National Intelligence Priorities Framework and the protection of American civil liberties and privacy, will conduct its foreign intelligence mission in accordance with the Constitution and with all governing legal authorities, including under FISA Section 702.

Foreign Efforts to Influence U.S. Elections

The most recent Annual Threat Assessment of the U.S. Intelligence Community, issued in March 2025, highlighted that Russia is still conducting operations "to influence U.S. elections" and also that "Moscow's malign influence activities will continue for the foreseeable future and will almost certainly increase in sophistication and volume." The Assessment further notes: "Moscow probably believes information operations efforts to influence U.S. elections are advantageous, regardless of whether they affect election outcomes, because reinforcing doubt in the integrity of the U.S. electoral system achieves one of its core objectives."

Separately, General Nakasone – who previously led the NSA and U.S. Cyber Command – publicly testified to Congress that U.S. Cyber Command conducted more than two dozen cyber operations targeting foreign threats to the 2020 election. He said these operations marked an important shift from "being a static to an active force" disrupting foreign interference in U.S. elections.

13. Do you share Gen. Nakasone's view that U.S. Cyber Command must be an "active force" in disrupting efforts by Russia and other U.S. adversaries to influence U.S. elections?

Any foreign attempt to undermine the American public's faith in our democratic process is a direct attack on the foundation of our nation and a core national security imperative. NSA and USCYBERCOM's continued focus on integrating operations, working across the U.S. government enables speed, scale and agility to persistently engage these adversaries to defend against foreign threats. USCYBERCOM's mission is to defend and advance U.S.

national interests in collaboration with partners and in accordance with the law. If confirmed, I will ensure any USCYBERCOM mission uses the full scope of the Command's operational authority while leveraging the expertise of the staff, including legal advisors and oversight professionals, and interagency partners, while vigilantly safeguarding civil liberties.

14. Do you commit, if confirmed, that you will do everything withing your authority as commander of U.S. Cyber Command and Director of the NSA, to protect the 2026 and 2028 U.S. elections from foreign interference?

The principles that have underpinned my entire military career are the protection of Americans, American values, and our homeland. I believe that elections are a central pillar of the American process of democracy. It's my understanding that NSA and USCYBERCOM persistently seek to provide critical foreign intelligence on and operate against foreign adversaries, including in their efforts to interfere with the electoral process. If confirmed, I commit to ensuring NSA and USCYBERCOM optimize the use of their respective legal authorities for the security of the nation, consistent with the National Intelligence Priorities Framework and the protection of privacy and civil liberties of its citizens.

15. Do you commit that you will do everything within your authority as Director of the NSA to warn and fully inform both this Committee and the American people of foreign efforts to influence U.S. elections?

If confirmed, I commit to keeping the committee fully and currently informed and to working with Congress and the Administration to share as much information as possible with the public— consistent with the protection of sources and methods—about NSA's mission, authorities, and oversight mechanisms.

16. Do you commit to appear before this committee – and also to direct NSA personnel to appear before this committee and to provide routine briefings to Committee staff – regarding foreign efforts to influence the 2026 and 2028 U.S. elections?

If confirmed, I commit to keeping the committee fully and currently informed of the Agency's foreign intelligence activities, including appearing before this committee and directing NSA personnel to appear, consistent with the Constitutional and statutory obligations of the Executive Branch.

Foreign Commercial Spyware

In 2023, Congress on a strong bipartisan basis passed legislation to combat the proliferation and misuse of foreign commercial spyware (*see* 50 U.S. Code § 3232a - Measures to mitigate counterintelligence threats from proliferation and use of foreign commercial spyware). Pub. L. 117–263, div. F, title LXIII, §6318(b), Dec. 23, 2022, 136 Stat. 3515 , provided that: "It shall be the policy of the United States to act decisively

against counterintelligence threats posed by foreign commercial spyware, as well as the individuals who lead entities selling foreign commercial spyware and who are reasonably believed to be involved, have been involved, or pose a significant risk to being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States."

17. Do you agree that the activities of foreign commercial spyware companies, as well as the activities of associated individuals and entities, pose a risk to the national security interests of the United States, including counterintelligence risks?

Yes, I agree. Foreign commercial spyware can pose significant national security and counterintelligence risks to the United States. Foreign commercial spyware companies' activities can facilitate intellectual property theft, compromise sensitive communications, and target U.S. government personnel and infrastructure.

18. Do you commit, if confirmed, to exercise all authorities available to you as NSA Director and Commander of U.S. Cyber Command to act decisively against the national security and counterintelligence threats posed by foreign commercial spyware?

If confirmed, I will ensure NSA and USCYBERCOM optimize the use of their respective legal authorities for the security of the nation and the protection of privacy and civil liberties of its citizens.

19. Do you commit, if confirmed, to work with this Committee to support additional measures to counter the national security and counterintelligence threats posed by foreign commercial spyware?

If confirmed, I will study this issue further and make recommendations to both the Executive and Legislative Branches.

20. Do you commit to comply with the statutory requirement for the Director of the NSA to submit to Congress on an annual basis, in coordination with the Director of the Central Intelligence Agency and the Director of the Federal Bureau of Investigation, a classified assessment of the counterintelligence threats and other risks to the national security of the United States posed by the proliferation of foreign commercial spyware?

Yes, if confirmed, I commit to working with the Executive Branch partners to comply with this statutory requirement.

21. Do you commit, if confirmed, to take all reasonable measures necessary to ensure that the NSA and U.S. Cyber Command comply with Executive Order (E.O.) 14093 Prohibition on Use by the United States Government of Commercial Spyware That

Poses Risks to National Security, and to also contribute to the Department of Defense's compliance with E.O. 14093? (*See* "Sec. 2. Prohibition on Operational Use. (a) Executive departments and agencies...shall not make operational use of commercial spyware where they determine, based on credible information, that such use poses significant counterintelligence or security risks to the United States Government or that the commercial spyware poses significant risks of improper use by a foreign government or foreign person.")

If confirmed, I will ensure NSA and USCYBERCOM comply with all Executive Orders, as applicable to those organizations.

22. Please provide any additional views that you have regarding the threat to U.S. national security posed by the proliferation and misuse of foreign commercial spyware.

The widespread availability of foreign commercial spyware offers powerful capabilities to a much broader range of state and non-state actors. This proliferation reduces the barrier to entry for our adversaries, giving them a low-cost tool to target our personnel, threaten sensitive operations, and act against our interests with little accountability.