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.