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.