SELECT COMMITTEE ON
INTELLIGENCE

UNITED STATES SENATE

Additional Prehearing Questions for

Lieutenant General Timothy D. Haugh

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?

If confirmed, my role is to lead one of the most consequential and impactful organizations to our nation's security. DIRNSA must be the best possible steward of the Nation's investment in NSA and create advantage for the Nation in competition, crisis, and contingency in each area of responsibility. Toward that end, the DIRNSA must ensure the health and effectiveness of NSA and its world-class employees in delivering outcomes against National priorities in foreign intelligence, cybersecurity, protecting our National Security Systems and providing combat support to the Department of Defense (DoD). I will build on my predecessor's priorities and focus on strengthening the workforce, ensuring a culture of compliance, investing to leverage new technologies, and focusing on threats facing the Nation, especially the pacing challenge posed by the People's Republic of China (PRC).

QUESTION 2: The congressional intelligence committees have supported the Intelligence Community's (IC's) evaluation of dual-hatting the Commander of U.S. Cyber Command and DIRNSA positions.

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

The signals intelligence (SIGINT) and cyber operating environments overlap. Therefore, the DIRNSA's roles in foreign intelligence, cybersecurity, and combat support would be adversely affected by cessation of the dual hat. Eliminating the dual hat would reduce NSA's visibility and understanding of CYBERCOM operations, increasing risk to NSA operational activities. Additionally, it would reduce the speed and effectiveness of cybersecurity collaboration in the protection of National Security Systems, the DODIN, and the Defense Industrial Base (DIB) by slowing and complicating information sharing and work with overlapping partners. Cessation of the dual hat would also complicate

relationships with Allies and partners that conduct both signals intelligence and cyberspace operations for their nations. Leaving the dual hat intact best ensures the protection of sensitive intelligence sources and methods, and best enables collaborative action in foreign intelligence, the protection of National Security Systems, and the cybersecurity of the nation.

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 intelligence and cyber operating environments intersect in an inextricable way. As a result, cessation of the dual hat would adversely affect USCYBERCOM. The Command's cyberspace operations would be less effective; de-confliction of the Command and the Agency's operations would be less efficient. Although the two organizations have documented working relationships and experience, termination of the dual hat would likely create complications in intelligence and military activities in the foreseeable future.

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.

The most positive aspect of the dual hat is the ability of a single decision maker, responsible for the separate and distinct mission outcomes of both organizations, to allocate resources, set priorities, and execute complementary actions to produce critical outcomes for the nation. It ensures that a single, fully informed decision maker is able to protect our nation's most sensitive signals intelligence equities and ensure both organizations are aligned with the nation's priorities. The Senior Steering Group that was commissioned to study the dual hat found that although there have been concerns in the past with respect to structure, budget, and oversight, any negative effects in these areas have been effectively mitigated by agreements and processes now in place to ensure clear accountability, cost reimbursement, and oversight. If confirmed, one of my priorities would be to ensure that the teams at

USCYBERCOM and NSA continue those best practices, and if necessary further build upon the activities that have made those agreements and processes effective thus far.

Being the head of an element of the IC and unified combatant command simultaneously would be no small task. Fortunately, I have had the opportunity to work closely with General Nakasone and witness his ability to balance time and priorities. I am very cognizant of the fact that each on its own is a demanding position, but surrounded by the right team, both can be done and done well.

QUESTION 3: What is your view on the dual-track supervision of NSA by the Secretary of Defense and the Director of National Intelligence?

The dual-track supervision of NSA by the SecDef and the DNI ensures appropriate transparency and oversight of NSA's missions as an element of the IC, the National Manager for National Security Systems and a leader in cybersecurity, as well as a combat support agency within the DoD. In my experience, the dual-track supervision of NSA is effective and ensures alignment with national and military requirements under clear executive guidance and direction, while setting the conditions through both OSD and ODNI for effective Congressional oversight.

QUESTION 4: How will you balance the four discrete responsibilities you will have to execute as the Director of NSA, the Chief of the Central Security Service, the Commander of U.S. Cyber Command, and the National Manager for National Security Systems?

While each of these important roles operate under discrete authorities with distinct chains of command, they have synergy in terms of shared operating environments and mission partners. The opportunity to create more effective and long-lasting outcomes through complementary activities is a powerful mission driver.

If confirmed, I will prioritize my time on the actions that enable the talented workforces of NSA, the Central Security Service, and USCYBERCOM to have the greatest impact on the nation’s security, while ensuring that each organization conducts its activities in conformance with the authorities and restrictions applicable to the organization’s specific assigned mission.

QUESTION 5: Please describe which of those roles do you believe is most important, and why. Please provide supporting details in your answer.

In my career of experience working with NSA and in my recent roles with USCYBERCOM, I fully understand the tremendous advantage NSA provides the nation. It is fundamental to all the other roles and its importance cannot be overstated. Our nation's success in each of these areas requires understanding of their essential interdependence and the overlapping operating domains of signals intelligence and cyber. If confirmed, my responsibility for the mission outcomes of each of these roles is to ensure that the national security interests of the United States will be the driver of my approach and decision making.

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

I am a career intelligence officer who has served 31 years in intelligence positions in the Air Force, the Joint Force, and the IC. I have commanded intelligence units at the Squadron, Wing, and Numbered Air Force level and served as a designated Senior Intelligence Officer in Special Operations, a Combatant Command, and multiple Air Force intelligence units in garrison or deployed. Initially trained as a Signals Intelligence officer, I have served in a total of seven intelligence assignments at NSA field sites, NSA headquarters, and within the Air Force's cryptologic component. In additional cyber assignments, I have been part of combined operations with NSA that allowed me to partner with or support NSA's Cybersecurity and SIGINT missions. I have been honored to serve with NSA for the majority of my career and have a deep appreciation for the incredibly talented NSA professionals that execute NSA's important missions in service of the nation.

I have immense respect for the current and former DIRNSAs. I have been fortunate to serve closely with the last three Directors; each has led transformational change at NSA with corresponding outcomes on the security of the nation. I have seen the impacts that leadership has on the culture, the workforce, and the mission.

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?

In my experience, NSA sets a high standard of integration, coordination, and collaboration with other IC agencies. If confirmed, I will further assess the current status of these relationships, and partner with other agency heads to identify further opportunities to improve integration and collaboration across the IC.

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

If confirmed, I will direct clear recognition across both organizations that each organization has separate roles, resources, and responsibilities and that our inter-service support agreements, memoranda of understanding, and special partnership agreements are followed and enforced.

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

If confirmed, I will be responsible for the mission outcomes of both organizations. I will prioritize the protection of our most sensitive equities and ensure decisions to set priorities, balance tradeoffs, and apply resources to mitigate risk to NSA equities and produce the best outcomes for the nation. In my experience there are also opportunities for CYBERCOM to contribute positively to NSA operations through the same intelligence operations cycle successfully employed in the other domains, which occurs when CYBERCOM operations generate new leads for NSA foreign intelligence collection.

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.

If confirmed, I will be committed to keeping the congressional intelligence committees fully and currently informed of NSA's intelligence activities. Congress has a critical oversight role of NSA's activities and NSA is required to provide appropriate information to committees with jurisdiction over NSA's activities. I will be committed to working with Members to understand the information they need to conduct their oversight.

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 -- fully and immediately.

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

It is not appropriate to withhold information that is within the jurisdiction of any Congressional committee. If confirmed, I will ensure that information is provided to the intelligence committees, to include following established procedures for briefing the most sensitive matters.

Functions and Responsibilities of the National Security Agency

QUESTION 13: What do you consider to be the most important missions of the NSA?

Both of NSA's principal missions, SIGINT and cybersecurity, are key to the safety and security of our Nation. The SIGINT mission plays a vital role in our national security by providing America's leaders with critical foreign intelligence they need to defend our country, save lives, and advance U.S. goals and alliances. The cybersecurity mission prevents and eradicates threats to U.S. National Security Systems with a focus on the DIB and the U.S. military's weapons. NSA's SIGINT and cybersecurity missions are also critical to fulfillment of NSA's combat support responsibilities.

QUESTION 14: How well do you think the NSA has performed recently in each of these missions?

Superbly – one of NSA's greatest strengths is its culture of mission focus, dedication, innovation, and continuous improvement. In my current role, I have been able to observe NSA's response to multiple recent crises; in each case providing an invaluable service to the nation.

QUESTION 15: If confirmed, what missions do you expect to direct the NSA to prioritize over others?

If confirmed, I would prioritize those foreign intelligence and cybersecurity missions concerning the pacing challenge of the People's Republic of China.

QUESTION 16: Every previous dual-hatted Director of NSA has experienced at least one major security incident under their leadership. What steps will you take to ensure this trend does not continue?

Ensuring the security of classified and other sensitive information handled or disseminated by NSA is vital. If confirmed, I would review past security incidents and the lessons from them. I would determine how these lessons have been applied across the NSA enterprise. I would then assess how conditions may have evolved so that NSA can anticipate new security threats. I will ensure continued investment in efforts to secure the NSA network and the enterprise, improved focus on processes and procedures that underpin the discipline of need-to-know, and proactive identification and mitigation of foreign intelligence and insider threats.

National Security Threats and Challenges Facing the Intelligence Community

QUESTION 17: What, in your view, are the current principal threats to national security most relevant to the NSA?

In my view, the principal threats to national security stem from the People's Republic of China, which continues to challenge the United States on a global scale while seeking to expand its malign influence, and Russia, which remains

engaged in unlawful military aggression in Ukraine and malicious cyber activity. However, threats to our Nation's security are numerous – actors such as Iran and North Korea attempt to coerce their respective regions with both conventional and cyber weapons, while terror groups, malicious cyber actors, and drug cartels present ongoing and transnational threats. Rapid changes in the technological environment will require the constant development of new and better approaches to collection, analysis, and dissemination of intelligence about these threats to maintain the safety of the Nation and our allies; this will be a priority for me if confirmed.

QUESTION 18: 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?

If confirmed, I will request an update on the impact that the spread of ubiquitous encryption is having on NSA's cybersecurity and SIGINT missions. Strong encryption undoubtedly advances cybersecurity but, in support of NSA's responsibility to collect and disseminate SIGINT, the Agency also has a responsibility to develop solutions to defeat foreign adversaries' use of encryption that hides their plans and intentions. NSA and other agencies have stated publicly that the increasing prevalence of encryption creates both challenges and opportunities for NSA's twin missions of SIGINT and cybersecurity. If confirmed, I would assess these challenges and the current resources that NSA has dedicated to addressing them.

QUESTION 19: Do you believe that the IC needs additional statutory authorities to address the proliferation of ubiquitous commercial encryption?

The existing authorities granted to the IC, and particularly the NSA, allow for the robust production of foreign intelligence of great value to the Nation while ensuring that the constitutional rights, civil liberties, and privacy of U.S. persons are protected. If confirmed, I want to assess how NSA makes use of its authorities and its biggest encryption challenges before formulating an answer on whether additional authorities would be beneficial. NSA needs to regularly evaluate its intelligence activities and optimize its use of the legal authorities and resources provided by Congress to ensure positive outcomes for the nation.

Foreign Intelligence Surveillance Act

QUESTION 20: Title VII of the Foreign Intelligence Surveillance Act (FISA) will sunset on December 31, 2023, including what is commonly known as Section 702. If Section 702 authorities were to end or even be diminished, what would be the impact on national security?

As a current customer of FISA Section 702 derived products, I recognize the value and the importance of this key authority in providing unique foreign intelligence to fulfill national priorities. From my experience in my current position, I believe that, if this authority were to sunset, there would be a significant detrimental effect on national security. It is my understanding that intelligence derived from Section 702 has been critical in counterterrorism, cybersecurity, counterintelligence, countering international drug trafficking, and strategic competition. It is also my understanding that one hundred percent of the President's intelligence priority topics reported on by NSA were supported by Section 702. However, I would defer to the White House, ODNI, DoD, and NSA leadership to fully characterize the value of this authority. If confirmed, I fully commit to working with Congress to ensure that surveillance conducted pursuant to Section 702, and all activities governed by FISA, are carried out consistent with the Constitution, U.S. law and policy.

QUESTION 21: Please describe why it necessary for NSA to have the ability to perform U.S. person queries of information acquired pursuant to Section 702 of FISA. What would the implications be in NSA was required to seek a warrant and probable cause prior to performing such queries?

Although I am generally familiar from sources such as the IC's Annual Statistical Transparency Reporting that NSA at times performs queries relating to U.S. persons, this is an issue I have limited familiarity with in my current role with USCYBERCOM. At this time, I defer to current NSA leadership to fully characterize this and other aspects of the current efforts taking place under this authority. If confirmed, I fully commit to working with Congress on all matters related to this important authority.

QUESTION 22: Please clarify what is meant by "incidental collection." Can the IC use this collection to target U.S. persons? If not, what value does incidental

collection have in the NSA's ability to protect our national security from counterterrorism and counterintelligence threats?

Incidental collection can occur when a witting or unwitting individual communicates with an approved foreign intelligence target. Noting that this section of questions relates to the Foreign Intelligence Surveillance Act, I'll add that my understanding is that under FAA Section 702, NSA may not intentionally target U.S. persons – Section 702 is used to target non-U.S. persons outside the U.S. for foreign intelligence purposes. However, in the course of that collection activity, there is sometimes incidental collection of U.S. person information. NSA and the broader IC have approved processes and procedures for minimization and querying to protect the privacy of U.S. persons. At this time, I defer to current NSA leadership to characterize the current efforts taking place under this authority, including details of the minimization procedures and other safeguards that protect U.S. person information that is incidentally acquired. If confirmed, I would develop a deeper familiarity with these safeguards and fully commit to working with Congress on all matters related to this important authority.

QUESTION 23: Please describe the compliance regime that the NSA has in place for its Section 702 collection authorities.

If confirmed, I will be in a better position to evaluate the specifics of NSA's Section 702 compliance and oversight systems. However, from my current vantage point I am aware that NSA has a robust compliance regime designed to ensure adherence to all statutory and procedural requirements, including those relating to Section 702. NSA has a dedicated corporate compliance organization, and has also instilled a culture of compliance within the entire workforce.

QUESTION 24: What compliance regime does U.S. Cyber Command have in place to ensure proper access to Section 702 collection?

NSA's mission compliance and intelligence oversight framework ensures compliant implementation of all Section 702 activities conducted under NSA authority, including those activities supported by authorized US Cyber Command personnel. NSA's policies, procedures, training, technical controls (including access controls), and incident reporting processes apply.

Cybersecurity

QUESTION 25: What role do you see for the NSA in defensive cybersecurity policies or actions? What role do you see for NSA in supporting any U.S. Government offensive cybersecurity policies or actions?

DIRNSA is also designated as the National Manager for National Security Systems. This position necessitates close collaboration with the NSS community, including USCYBERCOM, other DoD components, the IC, and Federal Civilian Executive Branch agencies such as the Cybersecurity and Infrastructure Security Agency, and the elements of the private sector who use NSS to drive cybersecurity improvements in response to emerging vulnerabilities and adversary activity. If confirmed, I will fulfill my responsibilities as the National Manager and ensure that NSS partners and cybersecurity customers that timely access to actionable cyber threat intelligence, as well as NSA's advice on cybersecurity best practices.

QUESTION 26: 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, to include NSA, play significant roles in protecting the United States, to include the U.S. commercial sector, from cybersecurity threats. Commercial and government cybersecurity challenges are varied and inextricably linked. These challenges range from preventing foreign adversaries from stealing U.S. intellectual property and sensitive military technology information, to defending or responding to malicious cyber activity and ransomware extortion that threaten both public and private networks underpinning the safety, economic security, and way of life for all U.S. citizens. Given this cascading and pacing threat, NSA devotes an entire directorate to the Agency's cybersecurity mission to ensure NSA is postured to contribute to the protection of NSS, the DoD, the DIB, and other customers of the Agency's cybersecurity products and services, which includes the dissemination of cyber threat intelligence.
In recent years I have witnessed NSA's development of significant private sector relationships with the DIB and service providers to the DIB in support of that role, and if confirmed, I would continue building and strengthening those relationships. That collaboration offers collateral benefit for the protection of commercial networks outside the DIB, but I intend also to ensure our analysis and production

mission enables CISA and our other close mission partners across the government to effectively fulfill their similar responsibilities across other sectors.

If confirmed, I will continue to focus on NSA's efforts with industry, academia, and government partners to integrate public and private cybersecurity cooperation.

QUESTION 27: 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?

I would expect that the primary responsibility for securing U.S. private sector networks resides within the private sector; however, the U.S. Government has a responsibility to share specific threats with the network owners. NSA has made substantial progress in ensuring network owners, public and private, have information that they can use to mitigate cybersecurity threats – including mitigation measures, and cyber threat indicators such as how the threat actor is linked to the activity or a technology vulnerability. It is my belief that information shared with the key stakeholders, including internet service providers, cloud service providers, cybersecurity incident response companies, and others in the ecosystem provides security at scale. If confirmed as DIRNSA, I will continue to lean forward on sharing unclassified threat information with the public.

QUESTION 28: Should NSA publish finished cybersecurity intelligence products? Why or why not?

I believe NSA should continue making cybersecurity intelligence products available to the public, consistent with the protection of sources and methods, given the Agency's role within the Executive Branch for cybersecurity. As a customer of NSA intelligence analysis products, I have frequently seen NSA called upon to represent the entire spectrum of cyber threats in an individual intelligence product, such as a Cyber Threat Assessment. In my opinion, these products are the gold standard for providing actionable cybersecurity information to those who need it at the lowest possible security classifications.

NSA Capabilities

QUESTION 29: What are your views concerning the quality of intelligence collection conducted by the NSA, and what is your assessment of the steps that have been taken to date to improve that collection?

From my perspective, the quality of NSA's intelligence collection is superb. Collection, exploitation, cryptanalysis, and signals analysis are foundational to the success of NSA's SIGINT and Cybersecurity missions. From my experience as an NSA partner and customer, I have seen firsthand that NSA effectively aligns its collection activities with the National Intelligence Priorities Framework while maintaining agility to respond to changes in priorities, mission requirements, shifts in target technology and crises.

QUESTION 30: If confirmed, what additional steps would you pursue to improve intelligence collection and what benchmarks will you use to judge the success of future collection efforts by the NSA?

If confirmed, I will review the investment and prioritization that NSA is making in its access, cryptanalysis, and signals analysis programs to ensure that NSA is able to continue to effectively execute its SIGINT and Cybersecurity missions. If confirmed, I will also utilize my role as the SIGINT Functional Manager to oversee the entire IC's SIGINT capabilities, processes, and resources to ensure that they are appropriately aligned and funded. If confirmed, I will leverage NSA's qualitative and quantitative assessment tools to assist with informing resource decision making.

QUESTION 31: What is your assessment of the quality of current NSA intelligence analysis?

Throughout my career I have benefitted greatly from NSA's SIGINT products and I can state, without reservation, that the nation is well-served by the dedicated work conducted by NSA's analytic workforce. In my current position, I receive access to a vast array of NSA reporting that is the result of robust training, tradecraft and subject matter expertise. NSA's analytic workforce develops deep insight into its foreign intelligence targets by utilizing all of its target knowledge, technical insight and linguistic expertise. If confirmed, I will continue NSA's

significant investment in its analytic personnel and ensure that those resources are aligned with the nation's security priorities.

QUESTION 32: 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 a world class workforce, which I believe is the key component to NSA's analytic production. In addition, I will ensure that NSA is making the necessary investments in the technical capabilities that are needed for its analytic production. NSA utilizes a number of technical tools to assess the value of its intelligence production; if confirmed, I will instruct my leadership team to use these qualitative and quantitative assessment tools to inform leadership decision-making and ensure that NSA's analytic efforts are properly aligned with customer priorities. Ultimately, I believe that NSA's analytic production is best judged by its IC, military and policymaker customers, therefore, if confirmed, I will prioritize engaging with NSA's intelligence customers so that I receive direct feedback.

QUESTION 33: What is your view of strategic analysis and its place within the NSA? Please include your views about what constitutes such analysis, what steps should be taken to ensure adequate strategic coverage of important issues, and what finished intelligence products NSA should produce.

NSA analysts' deep and continuous expertise in SIGINT and cybersecurity issues provides unique perspectives within the IC. The nation benefits from NSA's perspective and involvement in National Intelligence Council (NIC) and multi-agency produced analytic products. In my experience NSA's intelligence analysis has been high value but, if confirmed, I plan to engage with the Agency's intelligence customers to receive their direct feedback on the benefits they derive from the Agency's intelligence products, to include products that are based on or could be considered to contain "strategic" analysis.

QUESTION 34: What are your views on the role of foundational research to NSA's mission?

In my multiple roles within NSA and as a mission partner of NSA, I have witnessed and benefited from NSA's strong history of foundational research. NSA's gifted in-house research organization is comprised of a highly technical and talented workforce that aims to develop new and innovative techniques and technologies to support and enable its SIGINT and cybersecurity missions. I have also observed NSA's research endeavors and collaboration with academia, industry, and Allies as exceptional enablers. If confirmed, I look forward to the opportunity to assess and provide more informed recommendations on the issue, particularly as fielding of artificial intelligence and advanced computing research accelerates.

NSA Personnel

QUESTION 35: 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?

The principles that should guide the NSA in this area are those grounded in legal precedent and Executive Branch policy, such as accountability, efficiency, and consistency. If confirmed, I will continue to implement the relevant policy guidance from the DoD and the ODNI regarding the use of contractors in support of NSA's intelligence-related functions. Further, it is my view that the NSA benefits from a multi-sector workforce that is postured to adeptly meet mission requirements, effectuate savings to the taxpayer by utilizing contractors in appropriate roles, and ensure appropriate accountability through clear delineation of support functions. If confirmed, I will ensure that NSA leaders, at all levels, understand the proper roles and limitations of contractors in meeting the requirements of the NSA mission.

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

It is my experience that executive agencies within the DoD and the IC have successfully integrated contractors into support roles for their respective missions. At present, I lack deep insight into the particular needs and nuances of the NSA regarding contractor support. However, it

is my belief based on my past and present leadership experiences in the military that appropriate contractor support functions would likely include, for example, professional support services, engineering and technical services, information technology services, and facility 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. For example, an inherently governmental function at NSA might be the supervision and control of NSA employees. If confirmed, I will ensure that the NSA is acting consistently with the Office of Management and Budget's (OMB) general guidance concerning inherently governmental functions, as well as relevant DoD or ODNI policies and guidelines.

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

Appropriate consideration should be given to the cost of contractors versus government employees. It is my belief that it is critical to have the proper workforce mix between government and contractor employees, given the importance of the simultaneous need to maintain institutional knowledge, make efficient use of taxpayer dollars, enable NSA success through diversified and skilled personnel, and ensure accountability in the workforce. If confirmed, I intend to become acquainted with the respective costs and benefits of each at NSA, and will give careful consideration to this issue to ensure NSA achieves the appropriate balance in its workforce.

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

It is paramount that NSA's leaders possess a careful understanding of NSA's functional requirements and mission needs, as well as timely and accurate information regarding the composition of the workforce. Relatedly, it is important that clear policies be in place to enable NSA's leaders to understand which NSA functions are inherently governmental and not appropriate for contract personnel. It is also necessary to give due consideration to the costs and benefits associated with the utilization of each category of personnel within the workforce. If confirmed, I intend to explore this area further to determine whether any particular improvements, policies, or tools are required to ensure the appropriate balance of government civilians, military personnel, and contractors in NSA's workforce.

QUESTION 36: What is your assessment of the personnel accountability system in place at the NSA?

Having previously been a supervisor of NSA employees, I know that NSA has high expectations of its employees in regard to ethics and compliance, while also ensuring validation through supervision and technical implementation of personnel accountability systems. I am also aware that NSA's independent and Senate-confirmed Inspector General (IG) identifies and investigates potential instances of fraud, waste, abuse, and misconduct. In my current role, I do not have a current perspective on NSA personnel accountability systems; this is an area in which I will request updates if confirmed.

QUESTION 37: 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 any personnel accountability system, processes that are equitable and ensure due process must be in place. The independence of the IG is a fundamental part of guaranteeing those processes are executed appropriately. If confirmed, I will be in a better position to offer further analysis of existing NSA processes, and how those processes compare to those of other IC components.

Security Clearance Reform

QUESTION 38: What are your views on the security clearance process?

I am aware that the DNI has ongoing efforts to update and reform the security clearance process. I have participated in the transition from periodic to continuous evaluation and am encouraged by the transition. I support these initiatives and if confirmed, I look forward to working with key stakeholders to identify and leverage opportunities to streamline the process to ensure the efficient recruitment and hiring of an elite, trusted workforce.

QUESTION 39: If confirmed, what changes, if any, would you seek to make to this process?

I intend to fully support any update or reform that provides the opportunity to improve the security clearance process. In particular, examining areas that enable hiring and retention of the talented workforce NSA needs, while ensuring necessary security. If confirmed, I will be better able to evaluate and assess what changes, if any, would need to be made to this process.

QUESTION 40: Should civilians, military, and contractor personnel be held to the same security clearance and adjudication standards for access to NSA facilities, computer systems, and information?

Civilians, military, and contractor personnel should be held to security clearance and adjudication standards as required by public law, Executive Orders, and DoD and ODNI Directives.

Management of the National Security Agency

QUESTION 41: In what ways can DIRNSA achieve sufficient independence and distance from political considerations to serve the nation with objective and dispassionate intelligence collection and analysis?

If confirmed, I will continue NSA's long and exceptional tradition of providing accurate, timely, and non-partisan foreign intelligence to policymakers in any

administration. In particular, I will continue to support NSA's culture of rigorous and independent intelligence analysis where analysts are free to pursue their assessments wherever the facts lead them.

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

If confirmed, I will rely on my 31 years in intelligence positions in the Air Force, the Joint Force, and the IC —to include NSA—to ensure that NSA maintains its independence from political considerations. Specifically, I will make it clear to leaders throughout NSA that NSA must maintain its independence from political considerations in order to retain the trust of the Nation.

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

Throughout my 31 years in intelligence positions, I have always provided fact-based, objective assessments to decision makers. If confirmed, as DIRNSA I will ensure NSA analysts' conclusions are provided to Administration officials in the event there is a disconnect between public statements and the intelligence.

QUESTION 42: How would you resolve a situation in which the assessments of your analysts are at odds with the policy aspirations of the administration?

If confirmed, I would communicate NSA's objective assessments to policymakers, regardless of the administration's policy aspirations. Ultimately, it is the job of NSA and the IC to provide their objective assessments, judgments, and conclusions to policymakers.

QUESTION 43: What are your views of the current NSA culture and workforce?

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

NSA has an exceptional culture and workforce. The culture has been built on a foundation of mission focus and technical expertise combined with a commitment to the rule of law and protection of civil liberties. NSA's future success will also be determined by the Agency's ability to recruit, develop and retain the depth of talent across all of the Agency's missions and functions that enable the outcomes the nation needs from NSA.

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

If confirmed, this will be my highest priority focus area; NSA's strength is the talented workforce. I have observed NSA's approach to tap into talent across the nation; developing a diverse work force that includes the disabled and neurodiverse. NSA must ensure that an environment of dignity, respect and opportunity is nurtured and sustained. NSA offers a unique and dynamic mission, but the United States has also experienced rapid change in the nation's workforce, our education, and the way we work; the Agency must continue to adapt to an ever-changing environment.

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

I assess the relationship between the civilian and military NSA work force to be strong, but will need to continue to evolve based on the pacing challenge of the PRC. If confirmed, I will continue to strengthen the role of the Central Security Service and ensure the Services have a clear understanding of the demands of the mission and the need for continued evolution of the military cryptologic work force. I will also explore opportunities to expand NSA and Service partnership as we collectively seek to address the cryptologic demands driven by the PRC's military expansion.

Transparency

QUESTION 44: Do you believe that intelligence agencies need some level of transparency to ensure long-term public support for their activities?

Yes, I do. Public trust and support are necessary for the IC to continue to conduct its activities; transparency with Congress and the public is integral in gaining and maintaining that trust.

QUESTION 45: If confirmed, what would be your approach to transparency?

Transparency in the IC is a balancing act, since the IC cannot perform its mission effectively unless it protects its classified intelligence sources and methods from disclosure to the Nation's adversaries. However, maintaining public trust is essential for the IC to be successful in its foreign intelligence mission. If confirmed, I would leverage a multipronged approach to ensure appropriate and meaningful transparency.

First, the NSA must exercise candor with all overseers across the three branches of Government. Access to NSA information allows overseers a unique vantage point into NSA activities, allowing them to ensure on behalf of the public they represent that the Agency is carrying out its activities in a manner consistent with U.S. laws, policies, and American values.

Additionally, NSA must make available to the public information about its activities to the greatest extent possible. It is absolutely critical that this information sharing does not jeopardize sensitive sources and methods, but also that the amount and detail of information shared enhances public understanding, with the ultimate goal of defending the nation while continuously maintaining the public's trust.

Disclosures of Classified Information

QUESTION 46: In your view, does the NSA take appropriate precautions to protect classified information and prevent, deter, investigate, and punish unauthorized disclosures of classified information?

In my previous assignments with NSA, I have observed NSA's approach to protecting classified information adapt based on threats and availability of new technologies. From my vantage point in my current position, I believe that many appropriate precautions are in place; however, I am unable to make a fully

informed judgment of all of NSA practices at this time. If confirmed, I intend to evaluate the existing efforts to ensure the protection of NSA intelligence and equities, in order to identify any possible areas for improvement.

QUESTION 47: If confirmed, how will you ensure that appropriate and necessary precautions to protect classified information are maintained and improved, if necessary?

If confirmed, I will be able to better assess the current posture through examination of existing safeguards and discussion with security experts in order to identify what improvements, if any, are necessary; ensuring the protection of NSA capabilities and information will be among my top priorities. NSA has an incredibly important mission, and powerful capabilities to execute that mission; but the Agency must protect those capabilities in order for the public and the rest of the government to have confidence in it.

QUESTION 48: 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 are interrelated and align with the priorities that underpin all Agency operations. If confirmed, I will continue the drive to recruit and retain highly skilled and trusted individuals who are dedicated to the mission and understand the sensitivities and restrictions surrounding the information they use to carry out their duties. The efforts of these personnel are indispensable in effectuating the success of DIRNSA's core responsibilities: optimizing SIGINT

collection against critical adversaries to provide policymakers and military leaders with high value intelligence information, and ensuring the security of NSS.

QUESTION 49: How do you think that individuals who mishandle, intentionally or unintentionally, classified information should be dealt with?

National security information is classified based on the harm to the nation if disclosed. The unauthorized disclosure of intelligence has grave impacts; whether intentional or unintentional, the mishandling of classified information is an incredibly serious matter. Workplace discipline, including termination and revocation of security clearances, as well as criminal penalties are options that should be considered depending on the facts surrounding such violations.