Senate Armed Services Committee
Advance Policy Questions for Ronald Moultrie
Nominee to be Under Secretary of Defense for Intelligence and Security

Duties, Qualifications, and Relationships

1. **If confirmed as USD(I&S), what do you believe would be your most critical duties and responsibilities?**

   The Under Secretary of Defense for Intelligence and Security (USD(I&S)) is responsible for supporting the Secretary of Defense in discharging his intelligence and security responsibilities and authorities including under Title 10 and Title 50 of the United States Code.

   I understand that the responsibilities of the USD(I&S) are assigned in DoD Directive 5143.01 and include: serving as the Principal Staff Assistant and advisor regarding intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters; exercising authority, direction, and control on behalf of the Secretary of Defense over the Defense Intelligence Agency, the National Geospatial-intelligence Agency, the National Security Agency / Central Security Service, the National Reconnaissance Office, and the Defense Counterintelligence and Security Agency; establishing policy and priorities for, and providing oversight of, the defense intelligence and security enterprises; exercising oversight of personnel policy to ensure that intelligence organizations in the Department of Defense are staffed, organized, trained, and equipped to support the missions of the Department; ensuring that the DoD intelligence components that are also elements of the intelligence community are responsive to the Director of National Intelligence (DNI) in the execution of the DNI's authorities; ensuring that the combatant commanders, the Joint Chiefs of Staff, and the civilian leadership of the Department are provided with appropriate intelligence support; ensuring that counterintelligence activities in the Department are conducted and managed efficiently and effectively; ensuring that certain sensitive activities which the Department conducts or supports are conducted and managed efficiently and effectively; overseeing the implementation of assigned DoD security policies and programs to ensure efficiency and effectiveness; and serving as the Program Executive for the Military Intelligence Program.

2. **What is your understanding of the differences between the title 10 and title 50 duties of the USD(I&S)?**

   My understanding is that the USD(I&S) assists the Secretary of Defense in satisfying all of the Secretary's title 10 and title 50 statutory responsibilities in the areas of intelligence and security and that the duties of the USD(I&S) are prescribed in DoD Directive (DoDD) 5143.01.

Pursuant to subsection 3038(a) of title 50, the Secretary of Defense has the following responsibilities, which are to be conducted in consultation with the Director of National Intelligence: (1) ensure that the budgets of the intelligence community (IC) elements within the Department of Defense (DoD) are adequate to satisfy the overall DoD intelligence needs; (2) ensure appropriate implementation of the policies and resource decisions of the Director of National Intelligence by DoD Components within the National Intelligence Program (NIP); (3) ensure that DoD tactical intelligence activities complement and are compatible with intelligence activities under the NIP; (4) ensure that the IC elements within DoD are responsive and timely with respect to satisfying the needs of operational military forces; (5) eliminate waste and unnecessary duplication among the DoD intelligence activities; and (6) ensure that DoD intelligence activities are conducted jointly where appropriate.

3. **What leadership and management experience do you possess that you would apply to your service as USD(I&S), if confirmed?**

I have had the privilege of serving at the highest echelons of the Defense Intelligence Enterprise and the Intelligence Community. Serving over a combined 17 years as a member of the Defense Intelligence Senior Executive Service and the CIA's Senior Intelligence Service, I led some of our nation's most sensitive multi-intelligence missions and served with some of the most technically adept and dedicated professionals in the U.S. Government. Having served in leadership positions in operations, science and technology, staff and budget, legislative affairs, and joint organizations has enabled me to provide objective, time-sensitive intelligence to the warfighter, policy makers, and senior government leaders. As the Operations Director for the National Security Agency, I worked with many departments and agencies including across the Intelligence Community on critical challenges and established many trusted bilateral and multi-lateral foreign partnerships with our key allies.

If confirmed, I would use my coalition building skills and experience in the private sector to enable our nation to stay ahead of its adversaries. Also, I would continue to mentor the next generation of intelligence and security professionals. If confirmed, I would always serve with integrity while practicing servitude leadership. Lastly, I would use my decades of resource stewardship to ensure that the defense intelligence and security enterprise operates in an effective and efficient manner.

4. **Please provide an example of a situation in which you led and brought to conclusion a management improvement/change initiative in a complex organization.**

In a prior role as one of an agency's most senior operations leaders, I realized that the processes for after-hours and weekend decision-making lacked the content and authorization specificity needed to conduct operations. In coordination with the agency's senior leadership team, I crafted the inaugural guidance to establish governance framework for such decision-making. This guidance is employed globally today and enables the agency to identify, assess, and respond 24/7 to critical events worldwide, which in-turn enhances the quality and timeliness of intelligence provided to our government's most senior leaders.

5. What is your experience across the domain of intelligence matters? Security matters?

My career has been a series of foundational intelligence experiences and assignments each preparing me for additional responsibility. As a member of the U.S. Air Force, I trained as a linguist at the Defense Language Institute/Foreign Language Center and subsequently served a 3-year tour in Asia, which launched me on a professional intelligence trajectory. As a civilian leader at the National Security Agency (NSA), I addressed a wide spectrum of issues as I led NSA's efforts against several intelligence priorities. My responsibilities were comprehensive as I worked to satisfy intelligence requirements, served as the director of NSA's collection and processing organization, and led analytical and reporting efforts, culminating in my appointment as the director of operations. I was also a senior leader in the CIA's Science and Technology Directorate and had an important role while serving in the Office of the Director of National Intelligence (ODNI). I played a key role in advising the Secretary of the Navy on cybersecurity, emerging technology, and data issues.

I built strong relationships across the interagency working with the defense intelligence enterprise and organizations such as the ODNI, the Federal Bureau of Investigation, the Department of the Treasury, the U.S. Marshals Service, the Department of Homeland Security, and the Department of State Bureau of Intelligence and Research. I was selected to lead to major damage assessments and equity reviews of two of our nation's highest profile data compromises.

Lastly, I received a Master of Science of Strategic Intelligence (MSSI) degree in Russian studies from the National Intelligence University (NIU), the preeminent academic institution for the Intelligence Community. In 2020, I served as a member of the NIU's Board of Visitors, reportedly becoming the first graduate to ever to serve in this capacity.

6. Are there are any actions you would take to enhance your ability to perform the duties and exercise the powers of the USD(I&S)?

If confirmed, I would immediately begin to re-establish my close working relationships within the Pentagon, the ODNI, the other IC elements, and entire the Defense Intelligence Enterprise.

7. If confirmed, what specific duties might you expect the Secretary of Defense to prescribe for you, particularly in light of the lines of effort set forth in the 2018 National Defense Strategy (NDS)?

I believe my duties, aligned with the Secretary's 2021 Interim Defense Strategic Guidance, would include posturing the Defense Intelligence and Security Enterprises against the threat of China, countering Russia's malign influence activities, and the persistent regional threat posed by Iran and North Korea, while fostering the expansion of interagency cooperation and international partnerships to address national security priorities. Additionally, the Department must protect our personnel at home and abroad, a task that includes developing a collaborative and accountable culture that does not accept harassment or violent extremism within its military and civilian ranks.

8. **If confirmed, what duties and responsibilities would you assign to the Deputy Under Secretary of Defense for Intelligence & Security?**

   If confirmed and within the limits of policy and the law, I would ensure that the duties and responsibilities of the Deputy Under Secretary of Defense for Intelligence and Security are sufficiently broad such that my deputy would serve as a full partner.

9. **If confirmed, specifically what would you do to ensure that your tenure as USD(I&S) fulfills the fundamental requirement for civilian control of the Armed Forces embedded in the U.S. Constitution and other laws?**

   I am committed to civilian control of the Armed Forces in accordance with the U.S. Constitution and other applicable law. I recognize that the Department's civilian and military personnel together, with the support of DoD contractors, enable our mission success, and civilian control of the Armed Forces ensures accountability to the will of the people through our elected representatives.

10. **How do you view the relationship and division of responsibilities between the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) and the Office of the Director of National Intelligence (ODNI)? On what matters would you expect to collaborate with the ODNI, if confirmed?**

    I am aware that the OUSD(I&S) works closely with the Office of the Director of National Intelligence (ODNI). The partnership and integration between OUSD(I&S) and ODNI enables the Intelligence Community to deliver national intelligence support to policymakers and warfighters on threats to our national security.

    The USD(I&S) is dual-hatted as the Director of Defense Intelligence within the ODNI. There is also a military officer who serves as the DNI's Advisor on Military Affairs (DAMA). I believe their staffs coordinate to effectively and efficiently ensure quality intelligence is provided in support of our national leadership and warfighters. As a principal member of the Suitability and Security Clearance Performance Accountability Council (PAC), the USD(I&S) works with the DNI, who is the Security Executive Agent and also a principal member of the PAC.

11. **What is your understanding of the relationship and division of responsibilities between the OUSD(I&S) and the Office of the Under Secretary of Defense for Policy (OUSD(P)), particularly as regards policy and programs for information operations, including military deception and operations security (OPSEC)?**

My understanding is that the Under Secretary of Defense for Policy (USD(P)) is the Principal Staff Assistant for information operations.   I also understand that the USD(I&S) has responsibility for coordination of DoD IO activities with the Intelligence Community, as well as the development and implementation of DoD policy, programs, and guidance for DoD deception and operations security.

12. In your view, what would be the appropriate relationship between the USD(I&S) and the Chairman of the Joint Chiefs of Staff in regard to providing operational intelligence, counterintelligence, and security support to the warfighter?

I believe the relationship between the USD(I&S) and the Chairman of the Joint Chiefs of Staff is one of mutual support and consultation to ensure that the defense intelligence enterprise provides the warfighters with the best intelligence possible, which enables the Chairman to provide the best military advice to the Secretary of Defense.

13. How are responsibilities for the oversight of the activities and programs of special operations forces delineated between the OUSD(I&S) and the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD(SOLIC))?

I understand that USD(I&S) and the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD(SO/LIC)) acting together are the primary oversight officials for all Special Operations Forces (SOF) intelligence and intelligence-related activities and programs. If confirmed, I will partner with ASD(SO/LIC) to ensure that our oversight of SOF is coordinated and collaborative.

14. Are there any programs currently overseen by the OUSD(I&S) that would be more appropriately overseen by ASD(SOLIC), in your view?

I am unaware of any such programs. If confirmed, I will work closely with the ASD(SO/LIC) to ensure that together we provide the Secretary of Defense with the best organizational alignment to accomplish U.S. national security objectives.

15. How do you view the relationship and division of responsibilities between OUSD(I&S) and the Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSD(A&S)) in regard to both unclassified and classified contract efforts?

I understand the relationship between OUSD(I&S) and the Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSD(A&S)) is one of cooperation and collaboration. If confirmed, I look forward to partnering with the USD(A&S) to ensure that DoD acquisition programs receive the intelligence needed to acquire superior defense capabilities and that appropriate consideration is given to the central role of security throughout the acquisition process to protect the integrity of our acquisitions in the face of the persistent threat of compromise by our adversaries.

16. How do you view the relationship and division of responsibilities between the OUSD(I&S) and the DOD Chief Information Officer, particularly with respect to the cybersecurity mission; developing interoperability requirements applicable to information systems architectures for processing intelligence and counterintelligence information; and the certification of intelligence information systems?

I view the relationship between the OUSD(I&S) and the Department of Defense Chief Information Officer (DoD CIO) as one predicated on collaboration and partnership to ensure synchronization between security policy makers and information technology service providers. I understand that OUSD(I&S) is responsible for development and oversight of information security and physical security policy. The DoD CIO advises the Secretary of Defense on information technology, including national security systems and defense business systems, and develops DoD strategy and policy for all DoD information technology and information systems. If confirmed, I will ensure OUSD(I&S) maintains a close partnership with the DoD CIO to enable the necessary security architecture to protect intelligence and counterintelligence information while effectively enabling the mission.

17. What is your understanding of the relationship and division of responsibilities between the OUSD(I&S) and the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) for the Defense Civilian Intelligence Personnel System (DCIPS)? For the identification of DOD language capability requirements?

It is my understanding that the USD(I&S) develops the policies for the Defense Civilian Intelligence Personnel System in close coordination with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)). I also understand that USD(P&R) works with USD(I&S) and the intelligence community to set and prioritize DoD foreign language capability requirements. If confirmed, I will study the relationship between USD(I&S) and USD(P&R) in identifying DoD language capability requirements.

18. How do you view the relationship and division of responsibilities between the OUSD(I&S) and the heads of the Intelligence Components of the Military Departments?

I believe that the OUSD(I&S) staff works closely with the heads of the intelligence and counterintelligence components of the Military Departments. I understand that the USD(I&S) provides input to the Secretaries of the Military Departments on the duty performance of the senior intelligence officer within each Military Department.

The USD(I&S) is the Principal Staff Assistant to the Secretary of Defense with authority delegated from the Secretary of Defense to establish policy for defense intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters. The Directors for Defense Intelligence within the Office of the USD(I&S) (OUSD(I&S)) have specific programmatic responsibilities and support the Under Secretary in carrying out the responsibilities assigned and exercising the authorities delegated to the USD(I&S) by the Secretary of Defense.

The Secretaries of the Military Departments exercise authority, direction, and control over all components within their respective Departments. So the heads of the intelligence and counterintelligence components within the Military Departments are under the authority, direction, and control of the Secretary of the Military Department and subject to policy oversight of the OUSD(I&S).

19. What do you perceive to be the role of the OUSD(I&S) with regard to the Reserve Component intelligence elements of Military Services?

I understand that, in accordance with DoD Instruction 5143.01, which outlines the responsibilities and functions, relationships, and authorities of the USD(I&S), OUSD(I&S) develops and provides policy guidance, resource advocacy, and oversight for the integration of Reserve Component intelligence elements, and ensures the Department effectively employs and resources Reserve Component intelligence elements to best support the National Defense Strategy. The programmatic role of OUSD(I&S) is the same with respect to the Active and Reserve Components of the Military Services. Like the Active Components, the Reserve Components intelligence elements are under the authority, direction, and control of the Secretary of the relevant Military Department in which they are located and subject to policy oversight of the OUSD(I&S).

20. What is your understanding of the USD(I&S)'s responsibility and authority for the management and oversight of Military Intelligence Program (MIP) and National Intelligence Program (NIP) funding? How do the processes employed by the USD(I&S) in the execution of these responsibilities differ from the Planning, Programming, Budgeting, and Execution (PPBE) process applicable to all other DOD organizations and funding?

As the MIP Executive Agent, the USD(I&S) has management and oversight of the Military Intelligence Program (MIP). The USD(I&S), in his role as the Director of Defense Intelligence, has visibility into the NIP through participation in the Office of the Director of National Intelligence (ODNI) resource decision forums. Additionally, I understand that the DNI and the USD(I&S) jointly sign out intelligence programming guidance to closely synchronize NIP and MIP programs to ensure that the Department's priorities are communicated to the intelligence community. If confirmed, I will work closely with the ODNI in ensuring that DoD intelligence requirements are supported within the NIP budget.

With respect to the Planning, Programming, Budgeting, and Execution (PPBE) process, it is my understanding the USD(I&S) is a full participant in the Department's PPBE process and that military intelligence requirements compete with the other DoD requirements.

21. **If confirmed, specifically what actions would you take to develop and sustain an open, transparent, and productive relationship between Congress—the Senate Armed Services and Senate Appropriations Committees, in particular—and the OUSD(I&S) and the Defense Agencies under the authority, direction, and control of the USD(I&S)?**

    I am committed to assist the Secretary of Defense in sustaining an open, transparent, and productive relationship between the Department and Congress. If confirmed, I look forward to engaging with the defense oversight committees on a routine basis to explain the Department's defense intelligence, counterintelligence, security, sensitive activities, and other intelligence-related activities.

22. **If confirmed, what steps would you take to ensure both that this Committee is provided with the notifications required under provisions of title 10, U.S. Code, section 2723, and that any such notification is accurate, complete, and timely?**

    I am committed to fulfilling the USD(I&S)'s responsibility under DoD Directive 5143.01 to make determinations on behalf of the Secretary of Defense, except for those related to nuclear, chemical, and biological security, in consultation with the Director of National Intelligence and the Director of the Federal Bureau of Investigation, as appropriate, and to notify Congress, as required by section 2723. If confirmed, I will ensure such notifications are accurate, complete, and timely.

Major Challenges and Priorities

23. **What do you consider to be the most significant challenges you would face if confirmed as the USD(I&S) and what specific actions would you take to address each of these challenges?**

Rebuilding trust and establishing close working relationships between the USD(I&S) and DoD senior leaders would be among the most significant challenges. The rebuilding of trust and establishing close working relationships with senior leaders of foreign partners would also be a challenge and priority. If confirmed, I would engage in sustained outreach with these leaders on mutual priorities and objectives with the goal of developing a strategic dialogue and viable courses of action on key issues.

Supervision, and Oversight of the Defense Intelligence and Security Enterprise

The USD(I&S) is vested with responsibility for the overall direction and supervision of the Defense Intelligence and Security Enterprise in the execution of intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters across DOD. Subject to USD(I&S) oversight, responsibility for executing policies and programs in these domains vests primarily in the Military Departments and Services, elements of the Office of the Secretary of Defense, and the Defense Agencies.

24. **What is your understanding of the role of the OUSD(I&S) in coordinating the activities of the Defense Intelligence and Security Enterprise?**

    In my understanding, the USD(I&S) is responsible for ensuring the actions of all of these elements are integrated to meet the needs of the Department and the Nation. The USD(I&S) does so by issuing policy, ensuring compliance, exercising control over the Military Intelligence Program, coordinating with ODNI on the National Intelligence Program, and by leading development of decisions affecting the Defense Security and Security Enterprise.

25. **In your view, does the USD(I&S) have the authority, organizational structure, and resources to provide appropriate oversight of the Defense Intelligence and Security Enterprise? If not, what additional authorities or resources does the OUSD(I&S) require, in your view?**

    I believe that the USD(I&S) has sufficient authority to provide policy oversight of the Defense Intelligence and Security Enterprise. If confirmed, I will work with the OUSD(I&S) staff to determine if additional authorities or resources may be required and to standardize OUSD(I&S) practices for effective oversight.

National Defense Strategy

The 2018 NDS focused DOD on "great power competition and conflict" with China and Russia as the primary challenges with which the United States must contend, together with the imperative of deterring and countering rogue regimes like North Korea and Iran. Finally, the framework emphasizes the defeat of terrorist threats to the United States and the consolidation of gains in Iraq and Afghanistan, while moving to a "more resource sustainable" approach to counterterrorism.

26. **In your view, does the current NDS accurately assess the current strategic environment, including prioritization of the most critical and enduring threats to the national security of the United States and its allies? Please explain your answer.**

    I believe the 2018 National Defense Strategy helped consolidate a consensus around the importance of addressing the erosion of U.S. military advantage, in key strategic areas. I agree with Secretary Austin that China represents DoD's pacing threat, given its increasing scope and scale of military modernization, its aggressive behavior. The Department must also work to address advanced, persistent threats – such as Russia, Iran, North Korea, and VEOs. Additionally, I believe the Department must take steps to address the profound impact cross-cutting challenges, including climate change, COVID-19 and other biological threats, that will influence our national security.

27. **In your view, what role(s) must the Defense Intelligence and Security Enterprise play in the implementation of the NDS?**

The Defense Intelligence and Security Enterprise is a crucial pillar supporting the National Defense Strategy. The enterprise must support decision makers, help ensure decision advantage for the U.S. allies and partners and safeguard personnel, information, operations, resources, technologies, and facilities against a wide range of threats and challenges.

28. How would you assess the current readiness and capabilities of the Defense Intelligence and Security Enterprise to execute the NDS?

The Defense Intelligence and Security Enterprise serve is a crucial pillar supporting the National Defense Strategy (NDS). I understand that it is postured to support the Department's execution of the NDS. If confirmed, I will work with stakeholders to develop my own assessment of the enterprise's readiness and capabilities to execute the NDS.

29. Does the OUSD(I&S) have the analytic tools and expertise to assist you, if confirmed, in evaluating the readiness of the Defense Intelligence and Security Enterprise to engage effectively across the spectrum of challenges presented by the current strategic environment—from low intensity, gray-zone conflicts to protracted, high-intensity warfare with major-power rivals? Please explain your answer.

I understand that OUSD(I&S) possesses significant expertise to assist me in evaluating readiness. If confirmed, I will review and leverage the available decision-support analytic tools and develop standardized, metrics-based approaches to reliably assess, monitor, and evaluate the posture and performance of the enterprise to enable effective engagements across the spectrum of challenges and achieve desired outcomes.

30. What do you believe are the main resource or capability shortfalls that could hamper the Defense Intelligence and Security Enterprise's execution of the NDS?

It is my understanding that the Department has realigned Military Intelligence Program (MIP) resources to better support the National Defense Strategy (NDS). As the Department makes further adjustments to its warfighting capabilities to support the NDS, I expect this
will impose additional requirements on intelligence and security that will need to be addressed. If confirmed, I will work with the OSD(I&S) staff to identify promptly any obstaces likely to hamper execution of the Interim Guidance.

31. If confirmed, how would you propose to address any gaps or shortfalls in the ability of the Defense Intelligence and Security Enterprise to meet the demands placed on it by the NDS?

If confirmed, I will work across the Department to ensure any capability gaps and shortfalls are identified and resourced throughout the Planning, Programming, Budgeting, and Execution process.

32. **If confirmed, what changes or adjustments, if any, would you advise the Secretary of Defense to make in the Department's implementation of the 2018 NDS with respect to intelligence and security?**

    I am supportive of the tremendous efforts the Department has made to date in implementing the National Defense Strategy. If confirmed, once I am up to speed on efforts to execute the Defense Intelligence Strategy, I will develop recommendations for the Secretary of Defense. It is critical that all efforts continue to accelerate support to the Department's posture with China as the pacing challenge.

The NDS affirms that "[m]ore than any other nation, America can expand the competitive space, seizing the initiative to challenge our competitors where we possess advantages and they lack strength."

33. **What role can the Defense Intelligence and Security Enterprise play in "expand[ing] the competitive space," in your opinion?**

    The enterprise has a pivotal role in enabling the Department to expand the competitive space. It can help identify technologies, tools, tradecraft, skills, resources, and processes that the United States could use to create advantage relative to its competitors. The enterprise is also essential in safeguarding DoD personnel, information, operations, resources, technologies, and facilities against a wide range of threats and challenges. If confirmed, I will work with the Director of National Intelligence to ensure that DoD and the Intelligence Community are fully integrated to collectively seize that competitive space.

34. **Competing in the information space is a major concern as reflected in the "36-star" letter sent by nine U.S. Combatant Commanders to the Acting DNI via the USD(I&S) on January 15, 2020. If confirmed, what steps would you take help address this challenge to assist Combatant Commanders executing messaging and influence operations around the globe?**

    If confirmed, I will evaluate efforts to mitigate influence-related activities against key adversaries. I will also work to help prioritize resources to support operations in the information environment and participate in Intelligence Community focus groups to help drive key concepts related to these activities.

    I understand that in response to the 36-star memo, the Performing the Duty of the USD(I&S) and the Director of National Intelligence (DNI) have been examining how to improve upon current processes to use intelligence to counter malign influence operations against the United States, its allies, and its partners. If confirmed, I look forward to partnering closely with the DNI, the Combatant Commanders, and the Directors of the Combat Support Agencies to further those efforts in alignment with national policy objectives.

35. **What revisions or adjustments would you recommend that the Secretary of Defense make to the 2018 NDS? Please explain your answer.**

If confirmed, I will work with colleagues to ensure the Department considers geo-political shifts, intensifying competition with China, transnational threats (including climate change, COVID-19 and other biological threats), and the evolving technology landscape in its review and development of the next NDS.

<u>Strengthening Alliances and Attracting New Partners</u>

Mutually beneficial alliances and partnerships are crucial to U.S. success in competition and conflict against a great power. To this end, the NDS stresses the importance of strengthening existing U.S. alliances and partnerships, building or enhancing new ones, and promoting "mutual respect, responsibility, priorities, and accountability" in these relationships.

36. **How would you characterize your familiarity with the leadership of cooperative foreign defense establishments, the intelligence and security services of foreign governments, and intelligence and security-related international organizations?**

    My past experience in the Intelligence Community and the Department of Defense has afforded me familiarity with cooperative foreign governments, their defense, intelligence, and security services, and their leadership, as well as related international organizations. If confirmed, I look forward to strengthening U.S. ties with defense and intelligence counterparts around the globe, and collaborating on areas of shared interest and concern.

37. **If confirmed as USD(I&S), what specific actions would you take to strengthen and synchronize existing intelligence and counterintelligence relationships with foreign governments and international organizations?**

    I believe that allies and partners are force multipliers who bring a wealth of valuable and unique intelligence insight, access, and expertise to the partnerships.

    If confirmed, I commit to fostering strong defense intelligence and counterintelligence relationships with allies and partners focused on our shared concerns, including malign activities by China and Russia. I will work in close collaboration with our allies and partners to exchange valuable intelligence, synchronize our intelligence and counterintelligence efforts where mutually beneficial, implement economies of force, close intelligence gaps, and improve our overall understanding of the national and global security challenges that we face today.

38. **If confirmed, what factors would you consider in rendering decisions on the disclosure and release of intelligence to foreign governments and international organizations, including in support of combatant commanders' expressed desire for better intelligence and intelligence sharing to counter foreign malign activities?**

I understand that the National Disclosure Policy sets out the factors that must be weighed for the foreign disclosure of U.S. classified military information, including military intelligence. If confirmed, I would support combatant command requirements for military and national intelligence support to counter foreign malign activities. I agree broadly that the responsible foreign disclosure of military intelligence to friendly foreign governments and international organizations can further mutual defense and security objectives.

39. Do you agree with Admiral Davidson, the commander of U.S. Indo-Pacific Command (INDOPACOM), that his ability to strengthen alliances and partnerships would be greatly assisted by the funding of a "Mission Partner Environment" that would help provide a secure communications network with partners and allies throughout the region, similar to what exists in the U.S. European Command area of responsibility?

If confirmed, I will seek to get a better understanding of how the Mission Partner Environment Information Sharing Capability is being implemented pursuant to DoD Instruction 8110.01 within USINDOPACOM.

Joint Requirements Oversight Council (JROC) and the Joint Capabilities Integration and Development Systems (JCIDS)

Per section 181 of title 10, U.S. Code, the JROC is vested with the responsibility to assess joint military capabilities; establish and approve joint performance requirements that ensure interoperability between military capabilities; and identify new joint military capabilities based on advances in technology and concepts of operation. The JCIDS process was established to address overlap and duplication in Military Services' programs by providing the information the JROC needs to identify the capabilities and associated operational performance requirements needed by the joint warfighter.

40. How do you assess the effectiveness of the JROC and JCIDS in identifying and establishing joint warfighter capability requirements in the domains of military intelligence, counterintelligence, and security?

The JROC and Joint Capabilities Integration and Development System (JCIDS) use threat assessments from the Intelligence Community to inform Joint Force capability requirements and to guide requirements and capability development, including in the areas of military intelligence, counterintelligence, and security. The USD(I&S), as a statutory advisor to the JROC and its subordinate boards, provides advice that supports effective intelligence-related capability requirements and associated key performance parameters. If confirmed, I would closely coordinate with JROC members to ensure the JCIDS process continues to validate effective military intelligence, counterintelligence, and security requirements.

41. **In your view, have recent acquisition reforms that shifted authorities to the Military Services affected the JROC's ability to assess joint performance requirements in the military intelligence, counterintelligence, and security domains?**

    I understand that the recent reforms have transferred acquisition Milestone Decision Authority (MDA) from USD(A&S) to the Services, including for intelligence programs. One example is that the Air Force is now the MDA for the MIP-funded Next Generation Overhead Persistent Infrared satellites to provide missile warning. Changes in MDA, however, have not changed how DoD addresses requirements, as the Joint Capabilities Integration and Development System (JCIDS) process has not changed. The JROC continues to assess and validate effective joint performance requirements in the areas of military intelligence, counterintelligence, and security through its oversight of the JCIDS process, which still includes an Intelligence Support Certification that is required to complete the requirements validation process needed prior to an Acquisition Milestone Decision. If confirmed, I will work closely with JROC members to ensure the JCIDS process continues to validate effective military intelligence, counterintelligence, and security requirements.

The current Vice Chairman of the Joint Chiefs of Staff has emphasized joint and cross-domain capability requirements that the Military Services have not prioritized or are not responsible for developing, such as Joint All Domain Command and Control (JADC2). JADC2 demands ubiquitous interoperability, automated decision aids, and systems-of-systems integration.

42. **How would you ensure that the Defense combat support intelligence agencies and the National Reconnaissance Office comply with the JADC2 requirements promulgated by the JROC?**

    In addition to participating in both the Department and IC requirements development and system acquisition processes, OUSD(I&S) conducts an annual portfolio review to ensure MIP-funded efforts deliver the capabilities needed by the warfighters. If confirmed, I would work to ensure the OUSD(I&S) processes are working to provide the right data, to the right people, at the right time.

Given the role that National Reconnaissance Office (NRO) assets have in providing intelligence for warfighting functions, the JROC reviews NRO acquisition programs to ensure DOD requirements are being met.

43. **If confirmed, how would you ensure that NRO's close relationship with the JROC continues?**

    Consideration of both DOD and IC requirements is central to the USD(I&S) role. OUSD(I&S) facilitates the common gatekeeping function between the Joint Capabilities Integration and Development System (JCIDS) and the Intelligence Community Capability Requirements (ICCR) Process. If confirmed, I will work to maintain open communication throughout this process, and work closely with the Joint

Staff and Intelligence Community during the requirements validation process for NRO capabilities.

The streamlined middle-tier acquisition authorities enacted in Section 804 of the Fiscal Year (FY) 2016 National Defense Authorization Act (NDAA) sought to speed fielding of advanced technologies and systems.

44. What is your opinion of the effects of efforts to use of 804 authorities in intelligence-, counterintelligence-, or security-related acquisitions?

I believe that technological advances and development are outpacing DoD's ability to modernize and field capability using standard acquisition processes. Section 804 provides authority to the DoD to rapidly prototype and/or rapidly field capabilities under a new pathway, distinct from the traditional acquisition system. I understand this authority provides a pathway for the Defense Intelligence and Security Enterprises to develop, test, and field emerging technology to maintain pace with, or counter, adversary capability development.

Intelligence Support to the Warfighter

45. If confirmed, how would you balance the need for the combat support Defense intelligence agencies to provide intelligence support to the warfighter with the need to provide intelligence support to policy makers?

My understanding and belief is that balancing these needs will be one of my primary responsibilities. In today's environment of global and regional threats, most issues are relevant to both warfighting commands and policy makers. Where there are tactical and operational differences, if confirmed, I would work to ensure the DIE continues to satisfy requirements for operationally–relevant intelligence that directly enables warfighter success, and I would work collaboratively with policy makers to ensure the intelligence needs of senior national policymakers are met in order to support decision-making by our national leaders.

46. In your view, what opportunities exist across the Intelligence Community to improve intelligence support to the warfighter? If confirmed, what would you do to leverage these opportunities?

I believe in the importance of and the continued opportunity to improve collaboration across the Intelligence Community to better support the warfighter. If confirmed, I would engage early and often with the Combatant Commanders to improve my understanding of their needs, and I would frequently engage leaders within the Intelligence Community to obtain support to meet those warfighter needs.

47. If confirmed, what steps would you take to ensure that the geographic combatant commands are adequately assessing and prioritizing their intelligence needs?

It is my understanding that the OUSD(I&S) has multiple forums to engage with the Combatant Commands – for example, I understand there are monthly VTCs with all Combatant Command J2s. If confirmed, I will strive to ensure this and similar channels of communication are open and used routinely.

48. In your view, are the Joint Intelligence Operations Centers and Service Intelligence Centers organized and resourced to most effectively support warfighter requirements under the NDS, to include support to near-real time, multi-sensor joint detection, tracking, and targeting for the combatant commands? What changes may be required to optimize cooperative, cross-agency targeting support?

If confirmed, I will evaluate how to best resource the Combatant Command Joint Intelligence Operations Centers (JIOCs) and the Service Intelligence Centers (SICs) to support the NDS. I understand that some of the JIOCs are currently undergoing manpower studies to determine the appropriate manpower levels to meet the mission requirements of the Combatant Commands.

It would be incumbent upon the OUSD(I&S) to attempt to resource the Commands to help them meet their requirements, including in the area of targeting. If confirmed, I will support periodic reviews and re-alignment efforts to ensure priorities are met and resources effectively used to support the warfighter.

49. In your view, how are intelligence operations carried out by special operations forces different from those carried out by the Intelligence Community?

In general, the key difference is that these intelligence operations are conducted in direct support of special operations forces missions that support tactical operations. I understand that special operations missions require immediate and detailed intelligence to support operations that are executed on rapid timelines and in high-risk environments. In most cases, similar capability or capacity does not exist or is not readily available within the Intelligence Community or Department of Defense. I also understand other defense intelligence operations typically serve a more strategic purpose and reflect national priorities through its work as part of the Intelligence Community. While special operation forces generally conduct intelligence to directly support task forces conducting operations in support of the combatant commands, they are aware of national collection priorities and the strategic importance of their mission.

50. If confirmed, how would you work across the Defense Department, the Office of the Director of National Intelligence, and the CIA to ensure that intelligence activities carried out by special operations forces are properly coordinated with activities carried out by the Intelligence Community?

My understanding is that special operations forces intelligence activities are closely coordinated with the intelligence community as required by applicable law, policy, and agreements. If confirmed, I would continue to work closely with the ASD SO/LIC, Assistant to the Secretary of Defense for Intelligence Oversight, and other DoD senior intelligence officials to ensure special operations forces units comply with all applicable policies and directives. Additionally, I would welcome a continued dialogue with the committee to ensure clear and consistent reporting to the congressional oversight committees of intelligence activities carried out by special operations forces.

The OUSD(I&S) is charged to develop and oversee implementation of DOD strategy, programs, and policy for Intelligence, Surveillance, and Reconnaissance (ISR) capabilities and to integrate tasking, processing, exploitation, and dissemination (TPED) solutions.

51. Is the OUSD(I&S) participating in the JADC2 cross-functional team led by the Joint Staff J6? Do you intend to use the authorities delegated to the USD(I&S) to leverage information technology and innovative concepts to support the JADC2 initiative to develop an interoperable, joint command, control, communications, computer intelligence, surveillance, and reconnaissance architecture and capability to support the warfare of the future?

It is my understanding that the USD(I&S) is a full participant in the Department's Joint All Domain Command and Control (JADC2) initiative intended to connect distributed sensors, shooters, and data from and in all domains to all forces. If confirmed, I will continue to work closely with the DNI to shape required improvements to the C4ISR architecture to increase timely support to decision making at the strategic and operational levels.

In a February 27, 2020, *New York Times* Op-ed, Eric Schmidt, the chairman of the National Security Commission on Artificial Intelligence (NSCAI) and former chairman and CEO of Google, stated, "[i]f A.I. advances elsewhere outpace those of U.S. companies and the U.S. government, and give commercial and military advantages to our rivals, the resulting disadvantage to the United States could endanger U.S. national security and global stability. The same could be said for other emerging technologies." The report of the NSCAI emphasized this fundamental conclusion.

52. Do you agree that American pre-eminence in AI is critical for national and economic security? If confirmed, what priority would you assign to ensuring that the Defense intelligence enterprise invests in AI applications?

I agree that American pre-eminence in AI is critical for national and economic security. I concur with the NSCAI commissions' conclusion that "we must win the AI competition that is intensifying strategic competition with China."

The application of AI and algorithms are part of a class of data-centered capabilities that we must aggressively pursue to ensure DoD AI military dominance and information advantage in competition and conflict.

If confirmed, I will assign the highest priority to implementing data capabilities. I will also place emphasis on building AI training data to ensure we are turning our archived and daily intelligence into the data we need for the Department.

53. Do you agree that the Defense intelligence components should take maximum advantage of the foundational AI platform that the Joint Artificial Intelligence Center is sponsoring to develop AI applications for intelligence? If confirmed, what actions would you take to support this effort?

If confirmed, I will need more time to study this matter, but I believe Project Maven and other IC initiatives have built AI foundries that are operational today and were purpose-built for Defense Intelligence. I suspect those initiatives are much farther along, fitted more tightly to Defense Intelligence requirements and bring the speed and flexibility we need to bring AI at scale to our many intelligence data feeds. I will use the authorities granted to me in the Department of Defense Instruction (DODI) 5143.01 to weigh and assess the proper AI technologies Defense Intelligence requires.

54. What is your understanding of efforts by the OUSD(I&S) to develop and implement systems for the use of Artificial Intelligence to bring greater efficiencies to intelligence analysis, including opportunities to condense the time required by a human analyst to locate and prioritize potential targets and convert those observations to actionable intelligence for input to military decision making?

Speed, scale, and accuracy are USD(I&S) goals for transforming Defense Intelligence using data technologies such as AI. We want to be as early as possible on the sense-understand continuum to give us maximum time to respond to national threats. To achieve earlier warning and targeting time frames, we will rely on data technologies such as AI that make sense of data faster than humans. Machines will accomplish tasks that in the past needed humans to accomplish, such as extracting objects from imagery, or writing reports.

We envision a world where we globally surveil areas of interest hundreds of times per day and understand the smallest changes in seconds, and only machines equipped with AI will allow us to do this. Our product-focused approach to delivering intelligence will change from static, text-based artifacts to continuous data streams. Bringing forward these technologies at scale so that all Defense Intelligence sensors are first processed by accredited AIs and detections are then passed to humans for context, decision, and action will emerge as the new way of warfighting.

If confirmed, I look forward to presiding over these important transformations. Yet, I appreciate that achieving these results will require more than technology. Department leaders must also invest time to preside over the necessary human-centered changes that accompany the technology in order to guarantee successful adoption of these disruptive technologies.

Counterintelligence, Law Enforcement, and Security

55. What is your assessment of current and anticipated counterintelligence threats to DOD? Which threats do you assess to be the most concerning and why?

The Chinese and Russian intelligence services are the greatest foreign intelligence threats to the technological superiority and lethality of the Joint Force. I understand that China is using its intelligence services and proxies to threaten our military advantage by undermining our economic strength and innovation advantage through the wholesale theft of intellectual property and cutting-edge technology. I understand Russia is in a race to do the same and also intends to weaken American confidence in the U.S. Government and the U.S. military through sophisticated malign foreign influence campaigns.

56. What is your understanding of the roles and responsibilities of the OUSD(I&S) to provide strategic direction and oversight of implementation of counterintelligence policy, programs, guidance, and training to ensure they are responsive to validated DOD and national counterintelligence priorities? What changes, if any, in these roles and responsibilities would you recommend, if confirmed?

I understand the USD(I&S) has broad responsibility for oversight of DoD counterintelligence (CI). This includes development and oversight of Department CI policy, programs, guidance, and training of CI personnel. The USD(I&S) works closely with the Defense Intelligence Agency for development of CI strategies and supporting campaigns to ensure alignment with national level priorities. The USD(I&S) is a standing member of the National CI and Security Center's National CI Policy Board, and the National CI Strategy Board, and through these forums and related working groups, coordinates and collaborates within the U.S. Government. If confirmed, I will play an active role with my government counterparts to ensure the right balance of CI roles and responsibilities across the federal government.

57. In your view, how has the Department's security posture benefitted from the integration of the intelligence, counterintelligence, and law enforcement functions under the auspices of a single Under Secretary?

DoD faces complex security challenges and must adapt to changing threats and environments using targeted yet multidimensional mitigation strategies and countermeasures. Integrating policy oversight of intelligence, counterintelligence, and law enforcement, along with foundational security functions has enabled the Department to increase collaboration and leverage a wider variety of tools to respond to a given scenario. Our intelligence professionals and special agents strive every day to collect information, detect, and disrupt the capabilities, opportunities, and intentions of our adversaries. Working side by side with our security professionals allows them to develop effective policies, standard and repeatable procedures, and sufficient controls to deter, and deny our strategic competitors intentions. If confirmed, I will continue ensure that all communities under the authority direction and control of the Under Secretary continue to integrate seamlessly and continue to deny adversaries freedom of maneuver.

58. Does the integration of these functions under a single official raise civil liberties concerns? If so, what do you believe to be the most effective way to address those concerns?

No. I understand that integration of these functions within OUSD(I&S) provides uniform, Department-level oversight of these disciplines through alignment of policy, strategy, and resource prioritization. If confirmed, I will ensure that all intelligence and security activities, including counterintelligence and law enforcement are conducted throughout the Department in a manner that respects civil liberties and protect any right or privilege secured by the Constitution or the laws of the United States.

59. Does the USD(I&S) have adequate authorities and resources to execute the law enforcement policy function? If not, what additional authorities or resources are required, in your view?

I understand the law enforcement policy function resides within the Counterintelligence, Law Enforcement, and Security portfolio in USD(I&S), and that the staff is augmented with liaison officers and cleared contractors. Although I have not been briefed on the full range of current activities, if confirmed I will review this portfolio and ensure I&S has the right alignment of authorities and resources to perform the policy oversight function.

In the role of the DOD Senior Agency Official for Security, the USD(I&S) represents the Department on the Interagency Security Committee (ISC), created by President Clinton in 1995, six months after the Oklahoma City bombing, to develop security standards applicable to all non-military Federally-owned and leased facilities. *The Risk Management Process for Federal Facilities: An Interagency Committee Standard*, sets forth a number of "best practices" for determining a facility's security level and customizing physical security countermeasures.

60. In your view, has DOD benefitted from the adoption of any of the "best practices" endorsed by the ISC? Please explain your answer.

I believe that DoD has benefitted from the ISC's work. I believe this benefits DoD by keeping DoD's physical security standards for its leased spaces aligned with the physical security standards of other Federal leases, reducing build-out costs and reconstruction time when DoD moves into a space previously occupied by another Federal tenant. It also benefits DoD by better integrating DoD's security requirements into leased facilities DoD shares with other Federal tenants.

Personnel Security and Insider Threat

The USD(I&S) is accountable for managing and overseeing DOD's insider threat, personnel security, and the National Industrial Security programs. DOD has experienced devastating attacks from insider threats—attacks that have led to the death and injury of DOD personnel, as well as to the loss of highly-classified information critical to national security. The Secretary of Defense established the Department of Defense Insider Threat Management and Analysis Center (DITMAC) in 2014 to oversee the mitigation of insider threat risks to the Department and specific actions on insider threat cases. In November 2018, the National Insider Threat Task Force published the *Insider Threat Program Maturity Framework*.

Congress transferred responsibility for personnel security from the Office of Personnel Management to DOD at a time when a backlog of clearance investigations

reached near-crisis levels, while mandating that DOD transform the clearance process through modern data acquisition and continuous monitoring technologies. Congress also mandated that DOD significantly improve its abilities to support the integrity of the acquisition process by determining the beneficial ownership and responsibility determinations of companies and individuals with whom the Department contracts by applying similar continuous monitoring techniques. At the same time, the Department and Congress expect the intelligence and security components of DOD under the purview of the USD(I&S) to substantially increase the protection of the National Security Innovation Base from technology theft and subversion from foreign adversaries, while ensuring that American industry and academic institutions continue to be welcoming magnets for foreign personnel.

61. **Most of these very challenging new and enhanced requirements have been assigned to the Defense Counterintelligence and Security Agency (DCSA). What is your current assessment of the ability of DCSA to transform itself to meet these objectives?**

    I understand that the Department's intent for DCSA is to optimize the trustworthiness of the U.S. Government's workforce, the integrity of its cleared contractor support and the uncompromised nature of its technologies, services, and supply chains through vetting, industry engagement, counterintelligence support, and education. I further understand that DCSA has successfully merged three organizations, the Defense Security Service, the National Background Investigations Bureau and the Department of Defense Consolidated Adjudications Facility. The magnitude of what DCSA has already accomplished leads me to be optimistic that continued transformation of the agency to meet current and future critical technology protection requirements will remain on track.

62. **These DCSA-assigned missions are critical to DOD's innovation strategy led by the Under Secretaries of Defense for Acquisition and Sustainment and Research and Engineering. How would you ensure that DCSA is focused on meeting the needs of senior DOD officials outside of the OUSD(I&S)?**

    I understand that DCSA's Critical Technology Protection mission supports the agency's overarching responsibilities to protect national security by clearing industrial facilities, personnel and associated information systems and the DCSA serves as the primary interface between the federal government and industry providing daily oversight, advise and assistance to cleared companies and ultimately determining the ability of those companies to protect classified research, development, and delivery on behalf of the DoD and 33 other federal agencies. I understand the importance of their mission with A&S and R&E in protecting the Nation's critical technology. If confirmed, I will ensure that I&S and the leadership within DCSA are in constant collaboration with my counterparts within the Department and the Federal government.

63. **Specifically, if confirmed, how would you ensure that DCSA is highly responsive to the needs of the USD(A&S) for vetting DOD contractors in responsibility determinations?**

The Director, DCSA, operates under the authority, direction, and control of the USD(I&S). The timeliness of all background investigations conducted by DCSA will be closely monitored by USD(I&S) in cooperation with the Security and Suitability Executive Agents to ensure it meets its performance standards. To date, I understand that DCSA has greatly reduced the inventory and the amount of time it takes to conduct background investigations and expect the upcoming Trusted Workforce 2.0 will result in continued improvement in the timeliness of those investigations.

64. What is your understanding of the status of development, approval, and implementation of the Trusted Workforce 2.0 initiative?

I understand that the initial steps are already underway, and that I&S continues to work closely with the Security Executive Agent (SecEA), Suitability Executive Agent (SuitEA), and the Suitability and Security Clearance Performance Accountability Council (PAC) Performance Management Office (PMO) to complete development of Trusted Workforce 2.0 policy while working towards full implementation in the coming months. These efforts have included the enrollment of nearly all of the DoD cleared workforce in Continuous Evaluation (CE), which will enable the discontinuation of traditional and costly periodic reinvestigation practices.

65. What is your understanding of the remaining challenges in achieving reciprocity of clearances and access to classified information across government components and their contractors?

I understand that while significant strides have been made in reducing timelines for reciprocal security determinations, there is always room for further progress, and work force mobility continues to be a priority for the Department. I&S continues to work closely with the SecEA, the SuitEA, and federal partners to further refine policies related to reciprocity through Trusted Workforce 2.0, leverage technology to develop modern solutions for information sharing between agencies, and to oversee reform efforts as they are implemented.

66. How, if at all, should the Department change its data ownership and governance policies to facilitate DITMAC's ability to access data from, and make correlations across, the intelligence, counter-intelligence, law enforcement, physical security, personnel security, human resources, network monitoring, and cybersecurity organizations across the DOD?

Although I have not yet been fully briefed on all of these issues, I believe it is imperative that DITMAC and the DoD Insider Threat Enterprise have access to data from across these various relevant pillars to identify and mitigate potential threats from insiders, which will be especially critical as we modernize vetting to continuously review the trustworthiness of the workforce. If confirmed, I will ensure a continuous effort to eliminate stove-piping and remove barriers to data sharing, as allowed by law.

67. How should insider threat architecture and activities overseen by USD(I&S) be integrated and coordinated with the Department's cybersecurity architecture and activities, in your view? Can network activity monitoring for cybersecurity, especially on DOD's unclassified network, inform and augment insider threat detection? Can user activity monitoring for insider threat detection inform cybersecurity?

I understand I&S maintains a close relationship with the office of the DoD CIO, which fosters exceptional integration and collaboration relevant to insider threat, user activity monitoring, and cybersecurity. If confirmed, I will work to ensure this relationship continues and seek ways to enhance our efforts to find areas of common interest, force multiplication, and implement efficiencies across both mission of insider threat detection and cybersecurity.

68. In your view, does the OUSD(I&S) have the requisite authority and technical expertise to guide the development of a comprehensive capability that uses modern information technology to integrate all sources of information for identifying insider threats?

Although I have not yet been fully briefed on all of these programs, I believe the Department should maximize authorities and take a broad approach with respect to threat vector and population in the detection, prevention, and mitigation of an insider threat. This includes the technical capability to share data seamlessly between data sources. If confirmed, I will ensure a comprehensive Counter Insider Threat strategy and an innovative, directive approach, seeking to implement cutting edge data management policies and technologies that capture an "all source," shared picture of potential insider threats.

69. What is your understanding of the technical and systems integration challenges involved in improving personnel security processes and insider threat detection and prevention within DOD?

While I have not been briefed on the programs or challenges, I believe that DoD confronts the common challenges faced by many organizations when developing large scale information technology systems that ingest, disseminate, and retain large volumes of data with interfaces across numerous platforms and missions. However, if confirmed, I will endeavor to ensure the integration challenges are minimized and mission effectiveness in personnel security and insider threat is increased.

70. What is your understanding of the cultural and organizational resistance to improvements in the personnel security processes and insider threat detection and prevention in DOD?

I understand that the Department as a whole can be resistant to change due to its size, complexity, and culture. Although I have not yet been fully briefed on all of these issues, I believe any cultural or organizational resistance can be overcome by an emphasis on the benefit of increased security, conducted more efficiently and at an improved cost-to-benefit ratio, due to the improvement of current processes. If confirmed, I will continue to work toward overcoming the cultural and organizational resistance to forthcoming adjustments in these key security domains.

71. Given that several recent insider threats were from contractor employees, is it advisable and appropriate, in your view, for the DITMAC to have access to or be integrated in DOD contractors' data systems? If so, how might such a program be implemented? If such a program is not feasible, advisable, or suitable, what might you suggest as an alternative for mitigating the risk that contractor employees will engage in insider threat activities?

Effective sharing of information between the government and contractors is critical to our ability to collectively mitigate insider threats. Additionally, this enhances the vetting programs required for issuing forms of identification, which grant access to Federal facilities, as described in Homeland Security Presidential Directive-12. It is my understanding that the DITMAC serves an essential role as the over-arching DoD Insider Threat hub, and if confirmed I will examine more closely how DITMAC can be leveraged as an asset for additional insider threat mitigation and for strengthening connections with our industry partners.

72. In your view, how should DCSA posture the Department to deter, detect, and mitigate insider threats before they harm national security?

The designation and continuing transformation of DCSA brings together two national security missions instrumental to deterring, detecting, and mitigating threats to the Department – the continuous vetting of personnel and stand-alone programs throughout the DoD enterprise designed to counter threats posed by insiders. This convergence enables these separate but complementary missions to more easily share data, coordinate necessary actions, and streamline processes and capabilities to deter, detect, and mitigate insider threats. If confirmed, I look forward to working with DCSA to ensure this new organization reaches its full potential.

73. What can the OUSD(I&S) do to ensure that senior leaders in each DOD Component—not only the intelligence or counterintelligence communities—are fully invested in protecting their people, facilities, information from insider threats as a core mission objective?

A key component to detecting, preventing, and mitigating insider threats is ensuring management and leadership awareness of the risks to the Department and their role and responsibility in promoting awareness in the workforce. This includes ensuring that the organization's insider threat programs-- specifically programs responsible for determining suitability and fitness, issuing credentials, and vetting personnel-- meet requirements and are resourced for success in order to enhance and further such programs. It also means setting standards of conduct for the workforce, fostering positive workplace climates and cultures, and encouraging reporting of concerning behaviors and indicators. If confirmed, I will work with Senior Leaders across the Department to prioritize insider threat programs, including appropriate funding and resourcing to support this critical mission.

74. How should vetting policies and processes applicable to foreign military students enrolled in DOD training and educational programs help to mitigate risk to U.S. personnel, facilities, and equipment?

Following the terrorist attack at Naval Air Station Pensacola in December 2019, I understand that DoD took steps to more closely align vetting and security processes for international military students (IMS) and their accompanying family members with that of U.S. military personnel. In parallel with the implementation of these DoD-established installation security measures, I appreciate that relevant new U.S. law was enacted on January 1, 2021, as part of the National Defense Authorization Act for Fiscal Year 2021. Section 1090 of that Act was in response to the same terrorist attack. The new law requires DoD to establish vetting procedures as well as physical security requirements for non-U.S. individuals accepted for training on DoD installations in the United States. The implementation of the DoD requirements, as well as future implementation of the Section 1090 requirements will provide a greater level of security for both U.S. personnel and our allies and partners training with us on DoD installations. If confirmed, I will work to advance vetting policies and processes within the Department to help mitigate risks to U.S. personnel, facilities, and equipment.

The Department of Defense is pursuing a wide-ranging strategy to engage with commercial entities engaged in cutting-edge research and development. The Department recognizes that it needs new acquisition policies and practices to enable the Department to engage the private sector with the necessary speed, agility and flexibility. Two related obstacles are the time and difficulty involved in the security clearance process and the hurdles that non-traditional contractors face in getting access to data to test and demonstrate new information technology and software. The National Geospatial-Intelligence Agency (NGA), for example, concluded that it lacked the authority to share even its unclassified imagery data with companies and universities it hoped could develop dramatically improved exploitation capabilities through machine learning-based artificial intelligence algorithms.

75. How might DOD's security apparatus adapt and tailor its requirements and procedures better to support the Department's innovation activities, in your view?

The Department must overcome its reliance on traditional policies and practices when it comes to identifying and implementing innovation. Future Public-Private partnerships will be essential to the Department's innovation aspirations, and authorities can and should be changed if they inhibit creativity and progress provided those changes do not create unacceptable risk. Regarding background investigations, I understand there have been significant improvements in overall timeliness that should mitigate against delays in getting the right people on board. With respect to increasing collaboration with non-traditional contractors and academic researchers, I am aware of a range of initiatives underway in the Department that could help in this area. If confirmed, I will work closely with our Acquisition and Research colleagues in OSD and the Congress to continue to identify improvements in policy and oversight to ensure the Department is effectively engaged across the National Security Innovation Base.

Then-Secretary of Defense Mattis established the Protecting Critical Technology Task Force in late-2018, reporting to the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff. The Task Force was one component of DOD's response to Intelligence Community warnings that China and Russia are engaged in campaigns to steal trade secrets, proprietary information, and other forms of intellectual property from the United States, through infiltration of the software supply chain, acquisition of knowledge by foreign students at U.S. universities, and other nefarious means—all as part of a strategic technology acquisition program.

76. How would you characterize the threat posed by foreign nations to the integrity of the National Security Innovation Base? Which threats do you assess as most concerning, and why?

Although I have not been briefed on the details, I am aware from open source reporting that the threat is significant and concerning. I am aware that foreign nations are continuously probing our supply chains to identify and exploit weak links, poor or insufficient security practices, and insider threats. Threats that erode US technology superiority are of the highest concern given the negative effects they have on our ability to maintain a military advantage over future adversaries.

77. In your view, is the OUSD(I&S) appropriately resourced and organized to ensure the security of the National Security Innovation Base, critical technology, and related intellectual property that are critical to the DOD? What changes, if any, would you recommend?

Protecting the National Security Innovation Base requires tight collaboration across the Intelligence, Security, Acquisition, and Research enterprises within DoD, as well as equally strong collaboration with our interagency partners. Although I am not aware of any pressing resource or organizational challenges within I&S, if confirmed I will make it a priority to assess the full measure of support requirements and work closely across the enterprise to ensure we have the right alignment to counter the threat.

78. How would you propose to improve the support provided by the DCSA, the DOD counterintelligence organizations, and the national Intelligence Community to better protect the National Security Innovation Base, and enhance the Department's innovation strategy, especially with respect to technology companies that are non-traditional DOD contractors?

If confirmed, I will work to advance DoD counterintelligence, law enforcement, and security capabilities, leveraging DoD's interagency partners, especially the FBI, to detect, deter, and disrupt the attempts of China and other adversaries to penetrate and exploit the National Security Innovation Base and the Defense Industrial Base it supports.

Collection & Special Programs

79. In light of the rapidly evolving nature of the national security environment, to include significant advances by adversarial nations in the development and fielding of capabilities that could challenge DOD tradecraft, technologies, methodologies, and processes, what do you see as the most pressing challenges to DOD's ability to conduct technical and human intelligence collection activities?

It is clear the technology environment today has created pressing challenges in the conduct of traditional collection activities. Increasingly, adversary development of advanced technologies, such as computing, artificial intelligence, and secure communications, as well as the diffusion of sophisticated capabilities worldwide, complicate the information environment and reduce our national security advantage. In addition, the volume of commercially available data on individuals and their activity and the proliferation of both networked, correlated, and automated systems as well as algorithms that can exploit the information could pose a challenge to DoD human intelligence collection activities.

If confirmed, I would work to ensure that sufficient focus and resources are devoted to Defense Intelligence and Security Enterprise efforts to address these global realities and pursue additional resources if there are critical technical and human intelligence collection shortfalls. These challenges are not unique to the Department and, if confirmed, I would work with our IC partners to integrate and synchronize DoD and IC efforts and resources for addressing threats such as Ubiquitous Technical Surveillance (UTS), enabled by rapid advancements in artificial intelligence (AI) and machine learning (ML). Maintaining freedom of action in the physical or virtual world is paramount to the Department's ability to leverage all available collection platforms especially because cyberspace is now a contested domain. Our ability to collect in and through cyberspace must remain a priority. As with the physical domain, freedom in cyberspace is challenged by malign actors and the proliferation of AI and ML.

Lastly, I also believe that recruiting and retaining the right cultural and technical expertise is a challenge to overcome. Due to complex collection requirements, and the aggressive global posture of strategic competitors, with extensive CI capabilities we require a cadre of collectors that culturally understand, look, speak, and act like our adversaries wherever they challenge global norms. Diversity in the IC is a mission imperative—we must create a pathway that attracts the right individuals while not compromising the professional ethics that our enterprise is built upon.

80. If confirmed, how do you intend to approach these challenges to ensure that the DOD intelligence enterprise is postured to operate in an increasingly contested security and intelligence environment?

I believe the major challenges confronting the Department include adapting to and providing timely awareness and insights into a diverse, complex and ever-changing array of security challenges. If confirmed, I will lead the continuous review of processes and policies to support warfighters and decision makers in this changing environment. This may require changes in how DoD personnel train and use tradecraft, technologies, methodologies, as well as process adjustments for collection analysis. Aggressive efforts to ensure DoD is leveraging the best commercial technologies will remain essential, as will our ability to rapidly field technologies where required.

Intelligence Oversight

81. In your view, what is the role of the OUSD(I&S) in ensuring that sensitive activities across DOD are consistently conducted in accordance with standards of legality and propriety?

I understand the USD(I&S) is the Principal Staff Assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense regarding intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters. The USD(I&S) establishes policy and provides oversight and direction for the coordination, assessment, reporting, and conduct of Department of Defense (DoD) intelligence and intelligence-related sensitive activities, the Defense Cover Program, special communications, technical collection support to intelligence activities, defense sensitive support, and the clandestine use of technology. If confirmed, I would work closely with relevant defense and interagency stakeholders to ensure DoD sensitive activities are conducted consistent with law and DoD policy.

82. In your view, how should the OUSD(I&S) engage with the President's Intelligence Oversight Board and on what matters?

Based on my experience, the process in which the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)) notifies the PIOB of Questionable Intelligence Activities and Significant or Highly Sensitive Matters is effective. If confirmed, I look forward to fostering a positive relationship with the ATSD(IO) and PIOB during my tenure, and ensuring that my office provides subject-matter expertise, as required by DoD policy, to support the ATSD(IO)'s inspection, investigative, and reporting activities, including notifications to the PIOB.

Information Operations

The Russian government conducted, mainly through cyberspace, an aggressive information operations campaign against the United States in 2016 and again in 2020, in an attempt to influence presidential elections and undermine faith in America's democratic system and institutions. In 2016, in particular, DOD, and the Federal Government as a whole, were ill-prepared to detect, defend against, and respond to these operations.

83. What are your views on the roles, responsibilities, and preparedness of the Defense Intelligence and Security Enterprise to deter and defend against strategic information operations?

I believe that the Defense Intelligence Enterprise must improve its ability to compete in the information environment and to inform and shape the perceptions of specific audiences in order to gain or maintain a competitive advantage. My view is that the Department of Defense should conduct military operations in the information environment, including clandestine operations as defined in section 1631 of the National Defense Authorization Act for Fiscal Year 2020, across multiple domains to counter foreign malign actors and advance U.S. national security. Our efforts to deter and defend against foreign strategic information operations should be prioritized with appropriate resources and must include more robust coordination and collaboration across the Department, including the Under Secretary of Defense for Policy acting as the Secretary of Defense's Principal Information Operations Advisor, and the Executive Branch. If confirmed, I will work to ensure this happens.

Section 1631 of the FY2020 NDAA required the designation of a Principal Information Operations Advisor (PIOA) to the Secretary of Defense and a Joint Force Trainer and Joint Force Provider for Information Operations. The Secretary of Defense designated the USD(P) as the PIOA but the Committee is unaware that any Joint Force Provider/Trainer designation has been made. In addition, shortly before he left office, Acting Secretary of Defense Miller rescinded the PIOA designation and directed the creation in the Office of the Secretary of Defense of a Directorate for Strategic Competition, the Director of which would become PIOA and manage a task force. Acting Secretary Miller further directed the integration of the USD(I&S)-led Strategic Competition and Influence Task Force (SCITF) with the Directorate for Strategic Competition. The Committee has been informed that Acting Secretary Miller's decisions have been put on hold pending review and direction by Secretary Austin.

84. What are your views on the role that the OUSD(I&S) should play in the development and supervision of the implementation of Information Operations policy, strategy, and resource sponsorship? Should there be a separate Task Force on Strategic Competition and Influence in your view?

I understand that the Department continues to review its strategy, policy, and resources for information operations. I believe the USD(I&S) should play a key role in these efforts as the designated Principal Staff Assistant for certain information-related capabilities. If confirmed, I will work with the USD(P), the Chairman of the Joint Chiefs of Staff, and other DoD leaders to present the Secretary of Defense with the best possible organizational approach to address these issues.

85. What are your views regarding the designation of an Information Operations Joint Force Provider and Trainer?

I have not been briefed on this initiative, but if confirmed, I look forward to studying it in further detail.

On March 5, 2019, General Scaparrotti, then Commander, U.S. European Command, testified before the Senate Armed Services Committee that U.S. efforts to counter Russian influence operations still lacked "effective unification across the interagency" and that the United States has yet to develop "a multi-faceted strategy to counter Russia."

86. Do you agree with General Scaparrotti's assessment in this regard? Please explain your answer.

I agree that we must improve our interagency efforts to counter foreign malign influence. I understand that the Director of National Intelligence is establishing a Foreign Malign Influence and Response Center to improve the unified, whole-of-government effort to counter foreign malign influence from countries like Russia, China and Iran. If confirmed, I will ensure the USD(I&S) staff coordinates with this new Center and collaborates to ensure the Department's activities are synchronized, as appropriate.

87. In your view, how might the Defense Intelligence and Security Enterprise best contribute to efforts to counter Russian influence operations?

I understand the Defense Intelligence and Security Enterprise (DISE) is shifting its collection and other activities towards China and Russia. This includes the DISE contributing to efforts that counter Russian influence operations by developing frameworks that can be rapidly operationalized against key foreign target audiences to shape the collection focus and prioritization. If confirmed, I will continue to place emphasis on strategic competition with Russia and China and work to ensure DoD efforts are coordinated and integrated within a whole-of-government approach. I will also work to ensure appropriate planning, programming, and budgeting for DoD activities that are required to effectively engage in this mission space, such as foreign target audience analysis, key influencer identification, and early indicators & warnings of adversary disinformation.

In January 2020, nine combatant commanders sent a letter to the Director of National Intelligence requesting better and more timely support from the intelligence community to publicly illuminate malign influence and coercive activities by China and Russia.

88. In your view, how can the Defense Intelligence Enterprise better support the requirements of the combatant commanders?

I believe that the Defense Intelligence Enterprise must improve its ability to support combatant commanders by fully understanding adversarial goals in the information environment; by engaging with those who are impacted by foreign malign influence and coercive operations; and by enabling efforts, in alignment with national and defense priorities, to inform and shape the perceptions of specific foreign audiences to gain or maintain a competitive U.S. national security advantage.

89. In your view, would the illumination of these malign activities help to dissuade or deter China and Russia?

I believe DoD efforts to expose Russian and Chinese disinformation should be prioritized, supported, resourced, and executed to dissuade or deter their malign activities. If confirmed, I will make it a priority to attribute, expose, and counter foreign malign activities that harm U.S. national security interests.

In September 2018, DOD released its 2018 Cyber Strategy. The Strategy charges DOD to "defend forward, shape the day-to-day competition, and prepare for war" in the cyber domain.

90. In your view, what is the appropriate role for the Defense Intelligence and Security Enterprise in operationalizing the "defend forward, shape the day-to-day competition, and prepare for war" concepts animating the Department's 2018 Cyber Strategy?

These concepts require the DISE to provide intelligence support to DoD components at a speed and scale that enables current and future cyber operations. Therefore, I believe that intelligence support to cyberspace operations must accomplish the following objectives: supporting the Joint Force in execution of critical missions in a contested cyberspace domain; maximizing integrated information sharing and collaboration with foreign allies and partners, interagency stakeholders, and the public and private sectors; and normalizing intelligence support to cyberspace operations using business practices and processes similar to those used in other domains, while providing the DISE clarity of roles, missions, and functions in cyberspace operations.

DISE knowledge of the domestic risk landscape and work with the private sector informs DoD's defend forward efforts to preempt, defeat, and deter malicious cyber activity outside the U.S. that is, for example, targeting our critical infrastructure. DoD's "defend forward" operations also inform and guide efforts at DHS to anticipate adversary action, understand potential risks to critical infrastructure, and empower our private sector stakeholders with the information they need to secure their enterprise.

91. What actions would you take, if confirmed, to remediate any gap between Defense Intelligence and Security Enterprise capacity and capabilities and the goals of the Cyber Strategy?

If confirmed, I will work with Department stakeholders, the DISE, and IC to enable the continued implementation of the USD(I&S) Defense Intelligence Strategy for Cyberspace Operations. This strategy provides overarching direction to the DISE in closing gaps with the Cyber Strategy as identified in the 2018 Cyber Posture Review.

If confirmed, I would continue efforts to clarify intelligence roles and responsibilities to include those responsible for developing foundational military intelligence for cyberspace operations; incorporate and standardize cyber requirements into intelligence business processes and human capital management; develop the supporting infrastructure for optimizing and augmenting intelligence with advanced technologies, while continuing to support tool development; and emphasize the development of partnerships with allies and industry to include increased collaboration with the Defense Industrial Base and other government stakeholders in the Intelligence Community, law enforcement, and cybersecurity to improve intelligence support for whole of government operations.

92. What role should DOD, and the Defense Intelligence and Security Enterprise in particular, including the National Security Agency and the intelligence elements of United States Cyber Command, occupy in combating foreign influence operations, especially those conducted via social media?

I expect that foreign states will continue to use malign influence measures in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic process. If confirmed, I will work to ensure DoD and the DISE are postured to support the whole-of-government effort, using all elements of national power, to expose and counter clandestinely disseminated malign influence and information campaigns, propaganda, and disinformation.

93. What role should DOD and the Defense Intelligence and Security Enterprise in particular, play in anticipating or responding to cyber attacks on commercial entities, in your view?

DoD is responsible for threat response to DoD cyber incidents affecting DoD assets and the DoD Information Network (DoDIN). DoD can also support civil authorities for cyber incidents outside the DoDIN when requested by, for example, the Department of Homeland Security (DHS) when such support is approved by the appropriate DoD official, or directed by the President. Such support would be provided based upon the needs of the incident, the capabilities required, and the readiness of available forces. DoD, thru the DISE, actively characterizes and assesses foreign cybersecurity threats and informs relevant interagency partners of current and potential malicious cyber activity. Upon request, the DISE components may provide technical assistance to other U.S. departments and agencies. Other DoD Components may provide support to civil authorities in accordance with applicable law and policy.

94. What are your views as to whether the "dual hatting" of the Commander of U.S. Cyber Command as the Director of the National Security Agency should be maintained or terminated?

I understand that the Department, in coordination with the Director of National Intelligence, has been studying this question closely to ensure that any decision concerning the future of the dual-hat leadership arrangement is fully informed and addresses potential risks to national security and to the operational effectiveness of U.S. Cyber Command and the National Security Agency. I am also aware of the legal requirement for the Secretary of Defense and the Chairman of the Joint Chiefs of Staff to make certain certifications before this arrangement could be terminated. If confirmed, I would ensure that a review of this question is comprehensive so that decision-makers are fully informed about the impact on national security of any change to the dual-hat leadership arrangement.

95. Should intelligence support (under the oversight of OUSD(I&S)) to the overall DOD cybersecurity mission (under the oversight of the Principal Cyber Advisor) be enhanced, in your view? Please explain your answer.

I believe that a close and continuing partnership between the DoD Chief Information Officer, the Principal Cyber Advisor, and OUSD(I&S) is essential to best align intelligence policies and capabilities with policy objectives outlined in the DoD Cyber Strategy. I do not currently have sufficient information to have a perspective about the adequacy of the support at this time, but if confirmed, I will ensure OUSD(I&S) remains a valued partner in the DoD cybersecurity mission.

Torture and Enhanced Interrogation Techniques

96. Do you support the standards for detainee treatment specified in the revised Army Field Manual on Interrogations, FM 2-22.3, issued in September 2006, and in DOD Directive 2310.01E, *The Department of Defense Detainee Program*, dated August 19, 2014?

If confirmed, I will support the standards for detainee treatment in the Army Field Manual on Interrogations, FM 2-22.3, issued in September 2006, and in DoD Directive 2310.01E, DoD Detainee Program, dated August 19, 2014 (Incorporating Change 2, Effective September 18, 2020), and required by Section 1045 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92).

97. If confirmed, what role will you play in the ongoing triennial review and revision of FM 2-22.3 mandated by the NDAA for FY 2016?

If confirmed, I will work with the OUSD(I&S) staff to ensure that the review is thorough and that appropriate recommendations are provided to the Secretary. My understanding is that the review is examining the intelligence interrogation approaches and techniques in the FM based on lessons learned over the past several years.

98. Are there certain policies or processes set forth in FM 2-22.3 that in your view are in particular need of revision? Please explain your answer.

I am not currently aware of any provisions in the FM that may need to be revised, but if confirmed I will make my assessment.

Section 2441 of title 18, U.S. Code, defines grave breaches of common Article 3 of the Geneva Conventions, including torture and cruel and inhuman treatment.

99. **In your view, does section 2441 define these terms in a way that provides U.S. detainees in the custody of other nations, as well as foreign detainees in U.S. custody appropriate protections from abusive treatment?**

Yes. Section 2441 applies to war crimes, including grave breaches of Common Article 3 of the Geneva Conventions, committed by or against a member of the U.S. Armed Forces or a U.S. national. I believe that we must to continue to hold ourselves to the highest standards for the humane treatment of detainees, and that we must make clear to our foreign partners that we expect them to do the same.

<u>Imperative for Independent Intelligence Analysis</u>

100. **If confirmed, specifically what would you do to ensure that DOD intelligence analysts, including those seconded to offices that are not part of the defense intelligence structure, are independent and free of pressure from influence from their chain of command to reach a certain conclusion, including a conclusion that fits a particular policy preference?**

I believe that defense intelligence assessments must remain unbiased, objective, and free from political interference.

I understand that ensuring the objectivity of defense intelligence analysis is a critical part of the USD(I&S) oversight role. If confirmed, I will hold senior leaders of the Defense Intelligence Enterprise accountable to providing fact-based, unbiased analysis, independent of political factors in accordance with all applicable laws and professional standards.

<u>The Defense Intelligence Workforce</u>

The USD(I&S) exercises policy oversight of the Defense Civilian Intelligence Personnel System (DCIPS) to ensure that defense intelligence, counterintelligence, and security components are structured; manned; trained—including joint intelligence training, certification, education, and professional development; and equipped to execute their missions.

101. **Is the DOD civilian intelligence workforce properly sized, in your view? Please explain your answer.**

I have not yet had an opportunity to assess the size and capability of the defense civilian intelligence workforce, but I believe people are the most important part of any organization. If confirmed, I will work to ensure the Defense Intelligence Enterprise is sufficiently sized to provide timely and reasoned intelligence products to the warfighters and policy makers.

102. Does the DOD civilian intelligence workforce have the appropriate capabilities, and are those capabilities properly distributed, in your view?

I do not have sufficient information to provide a perspective at this time. However, based on my experience in intelligence, and particularly my time at the National Security Agency, it is my impression that the Defense Intelligence Enterprise is providing quality and timely intelligence to the warfighter and policy maker. However, as with any organization, missions evolve and adjustments to the workforce may be needed. If confirmed, I will work to assess our workforce alignment to national defense priorities and propose such actions as may be deemed beneficial.

103. Are the number and quality of candidates referred and available for consideration and selection by intelligence, counterintelligence, and security community hiring officials adequate to sustain and enhance the capabilities of the civilian intelligence workforce?

I have not received any information on candidate pools. However, I believe people are the most important part of any organization. If confirmed, I will work to ensure we have the most qualified intelligence and security professionals, and that we persistently and aggressively seek opportunities to expand candidate pools to acquire both the skills and diversity necessary to accomplish DoD intelligence and security missions.

104. If confirmed, what factors and characteristics would be most important to you in selecting a candidate for appointment in the Defense Intelligence Senior Executive Service (DISES)? As a Defense Intelligence Senior Level (DISL) official?

The Defense Intelligence Senior Executive Service (DISES) provides the executive leadership for the Defense Intelligence and Security Enterprise. I believe the Senior Executives Service Core Qualifications – Leading Change, Leading People, Results Driven, Business Acumen, and Building Coalitions – provide a sound underlying basis for executive selections. I believe there should be a premium placed on a proven ability to collaborate effectively across boundaries.

Defense Intelligence Senior Level (DISL) employees complement the executive leadership of DISES by providing the extraordinary substantive and technical expertise, in combination with the demonstrated talent for personal leadership, within critical career fields. If confirmed, I will continue to focus on identifying, selecting, and developing all personnel to accomplish our mission objectives, including DISES and DISL.

105. If confirmed, how would you go about ensuring that DISES and DISL under your authority are held accountable for both organizational performance and the rigorous performance management of their subordinate employees?

We can accomplish what we can measure. If confirmed, I intend to use the executive performance management system to maintain oversight of executive and senior level performance.

106. Are you satisfied with the subject matter and rigor of DISES and DISL professional development programs currently available across DOD? If not, what changes would you make to these programs, if confirmed?

I have not yet been briefed on the content and rigor of these professional development programs within DoD. However, if confirmed, I intend to assess the effectiveness of these programs. I believe that a talented and effective leadership cadre is critical to successfully delivering quality intelligence to the warfighter and policy maker.

107. Are you satisfied that the process employed by the OUSD(I&S) to validate whether a vacant DISES/DISL position should be rehired, restructured, or eliminated is effective in responding to current and emergent mission needs of the Defense Intelligence and Security Enterprise? If confirmed as the USD(I&S), what would be your role in this process?

I have not yet been fully briefed on the processes in place for validation of DISES and DISL positions. However, I recognize that continuous evaluation of requirements is an essential mechanism to ensure our leadership positions are appropriately manned and structured. Every executive wants maximum flexibility to adapt their organization to support mission success, and if confirmed, I will ensure oversight processes are in place that support an agile and adaptive Defense Intelligence and Security Enterprise.

The Intelligence Community "Joint Duty" program was established in response to the requirements set forth in the 2004 Intelligence Reform and Terrorism Prevention Act that service in more than one IC element be a condition for promotion to the senior executive level.

108. Do members of the DOD civilian intelligence workforce participate in the "Joint Duty" program? If so, to what extent does DOD participate?

I understand that the DoD civilian intelligence workforce participates fully in the Joint Duty program. DoD Instruction 1400.36 implements the Joint Intelligence Community Duty Assignment (JDA) Program within the Department and provides that JDA Program certification is a requirement for DISL and DISES positions. It is also my understanding that joint duty is encouraged in all defense intelligence components as a key element of an individual's career development.

109. What are your views on the merit and utility of the "Joint Duty" program as a professional development experience for members of the DOD civilian intelligence workforce?

I believe the civilian joint duty program is an essential element of the professional development experience for members of the DoD civilian intelligence workforce. It is key that our civilian intelligence professionals understand the relationships among the members of the intelligence community and that throughout their careers they build deep and enduring professional relationships across the Intelligence Community (IC). Joint experience supports a fully integrated and collaborative intelligence community. Similar to the way that the military joint duty requirements from the Goldwater-Nichols Act has paid dividends for the military services, the civilian joint duty program is vital to building a more integrated, interoperable, and effective IC.

110. What other innovative ideas do you have for the professional development of non-executive members of the DOD civilian intelligence workforce?

At this time, I do not have the requisite information about current efforts to recommend specific ideas. I believe that continuing professional development throughout one's career is critical to both developing the most effective intelligence capabilities and retaining the expertise behind it. Based on my experience at NSA, I believe that if we are to maintain our competitive advantage, we will need to build more effective public-private partnerships, both with academia and industry. We must find ways to enable seamless mobility between government and the private sector throughout an employee's career, particularly in out most demanding technical areas, to ensure we have the expert, professional, and motivated workforce the 21st century demands. If confirmed, I will pursue efforts to increase opportunities for professional development within the workforce that enable the career mobility necessary to build the diversity and capability of the workforce.

111. Is the DOD civilian intelligence workforce prepared to sustain requisite capacity and capability during the impending workforce "bath tub"—a descriptor often used to graphically illustrate the impending potential loss of civilian workforce expertise due to the retirement of large numbers of "baby boomers" and the lack of experienced people to fill the vacancies?

I have not been fully briefed on all aspects of the DoD civilian intelligence workforce hiring and personnel authorities. For any organization, understanding the dynamics of the workforce through effective workforce analytics is critical to plan for workforce requirement changes driven by evolution of mission—we must measure what we intend to achieve. If confirmed, I would ensure the OUSD(I&S) is taking necessary efforts to require active succession planning for the enterprise while aggressively projecting workforce requirements and that the authorities provided to the Secretary of Defense for the defense intelligence workforce provide the flexibilities necessary to address, maintain, and build workforce capability.

112. Does the USD(I&S) need additional hiring, development, recruitment, retention, or compensation authorities to enable further improvements in the capacity and capability of the DCIPS? Please explain your answer.

In general, I understand that the authorities under title 10 provide the Department with flexibility to address capacity and capability requirements of the civilian workforce. However, I am also aware that challenges continue to exist in DoD's ability to address competitive requirements for certain key skill areas, such as those in the cyber and STEM fields. I understand that the Department has limited pay authorities applicable to the National Security Agency needed to address a critical compensation shortfall in their cyber workforce. If confirmed, I will review the authorities available to the Department and assess whether any additional authorities are required to address DCIPS challenges.

Whistleblower Protection

Section 1034 of title 10, U.S. Code, prohibits taking or threatening to take an unfavorable personnel action against a member of the armed forces in retaliation for making a protected communication. Section 2302 of title 5, U.S. Code, provides similar protections to Federal civilian employees. By definition, protected communications include communications to certain individuals and organizations outside of the chain of command, including the Congress.

113. If confirmed, what actions would you take to ensure that military and civilian members of the Defense Intelligence and Security Enterprise who report fraud, waste, and abuse, or gross mismanagement—including in classified programs—to appropriate authorities within or outside the chain of command—are protected from reprisal and retaliation, including from the very highest levels of DOD and the broader Intelligence Community?

If confirmed, I am committed to ensuring protections are afforded to DISE personnel who report fraud, waste, and abuse, or gross mismanagement, in a manner consistent with law and regulation. Additionally, I will ensure that personnel who pursue retaliatory actions upon protected personnel are addressed appropriately, as established by law and regulation.

114. If confirmed, what role would you play in ensuring consistency in the application and interpretation of whistleblower protections across the Defense Intelligence and Security Enterprise?

If confirmed, I will carry out my responsibilities to ensure that the DoD policy implementing such protections is applied consistently and uniformly in accordance with law.

Sexual Harassment

In responding to the 2018 ODOD Civilian Employee Workplace and Gender Relations survey, approximately 17717.7 percent of female and 5.88 percent of male DOD employees indicated that they had edexperienced sexual harassment and/or gender discrimination by "someone atat work" in the 12 months prior to completing the survey.

115. If confirmed, what actions would you take were you to receive or otherwise become aware of a complaint of sexual harassment or discrimination from an employee of the OUSD(I&S)?

There is no place for this conduct in the Department of Defense or Intelligence Community. If confirmed, I will exercise my oversight responsibilities for the Defense Intelligence and Security Enterprise to ensure that reports of sexual harassment or gender discrimination are dealt with swiftly and in accordance with law and policy.

Space

In the past two years the United States has stood up the U.S. Space Command (SPACECOM) and assigned it responsibility for the operational planning of DOD space missions and activities. As well, the U.S. Space Force was established as a sixth Military Service, charged with the Title 10 responsibilities for the space domain.

116. If confirmed, specifically what would be your approach to enhancing the interface and synchronization of space-based capabilities resident in the Intelligence Community with military space organizations?

The DoD and IC have a long history of collaboration in fielding and operating space systems, and USD(I&S) plays an important role in the synchronization of these efforts. Space system development and operations benefits from collaboration across agency boundaries and the
effectiveness of those systems improves with improved integration. If confirmed, I will continue to look for opportunities to expand collaboration between NRO and other military space organizations to enable sharing of capabilities that are mutually beneficial to DoD and IC.

117. How would you recommend deconflicting tasking requirements in the space warfighting domain across DOD with tasking requirements from Intelligence Community customers?

Deconfliction for tasking intelligence collection is executed through the Functional Manager roles, which consider both DoD and IC priorities. As with other domains, intelligence support to space warfighting requires balancing tasking requirements among the numerous stakeholders served by national collection. There will likely be growth in the collection and analytical needs of space intelligence and defense missions and, if confirmed, I will work with the functional managers on ways to better streamline the tasking process to increase access, agility, and responsiveness to best satisfy these unique space intelligence requirements.

NRO recently signed a Memorandum of Understanding with the U.S. Army for a tactical space layer to provide alternative Position, Navigation and Timing, as well to provide Army ground stations with tactical battlefield situational awareness and ISR.

118. In your view, is the NRO moving to more of a direct support role to the Services?

The NRO provides critical intelligence to the Services to meet tactical to strategic requirements. I understand that NRO is working diligently to develop advanced space capabilities and resilient architectures to provide real time support to the warfighter. If confirmed, I will work with the NRO and the Department to develop end-to-end space architectures that can meet National, Service and Combatant Command requirements.

119. If confirmed, how would you ensure the Space Force and NRO are not duplicating capabilities and responsibilities for the Joint Force?

My understanding is that there is strong coordination between the Space Force and NRO which is reinforced through the mature DoD Budgeting Programming and requirements process. The USD(I&S) participates in these requirements through validation, resourcing, and oversight processes. If confirmed, I will ensure OUSD(I&S) has a continued active role in these processes

120. In your view, in a time of conflict in space, is unity of command, unity of effort, or some other approach the most effective in ensuring the protection and defense of U.S. Government and allied space assets? Please explain your answer.

The key to an effective "protect and defend" strategy is the seamless execution of space defense actions, synchronized across DoD and IC platforms under a collaborative unity of effort. The National Space Defense Center is where this unified defense comes together. As adversaries increasingly threaten US freedom of action in space, the DoD and IC must continue to strengthen partnerships to maintain a competitive advantage. Enhanced space cooperation within the U.S. Government and with the international community and commercial sector will provide a durable strategic advantage for the U.S. and our allies and partners and serve as a force multiplier to protect and defend against adversary use of space for purposes hostile to U.S. interests.

I believe that we succeed when we train as we intend to fight. Wargames, exercises, and planning activities continue to inform the development of space protect-and-defend tactics, techniques, and procedures. DoD is committed to an approach to space defense that balances the need to protect national space assets and continue the space-based intelligence mission that is critical to win in space and in support of other domains.

121. How best could members of the defense intelligence workforce—both military and civilian—be utilized in support of the U.S. Space Force?

The defense intelligence workforce offers a variety of capabilities to the U.S. Space Force (USSF), including intelligence support to space, technical and acquisitions expertise, and satellite operations. The Defense Intelligence Enterprise will continue to align resources and manpower to support the USSF in response to current and future space threats and enable effective deterrence and defense. If confirmed, I will work with the Department and across the IC to ensure the Space Force has access to intelligence personnel and capabilities.

The NRO is the only defense intelligence agency not designated as a combat support agency (CSA). Historically, the NRO has asserted that it should not be designated as a CSA because it does not make operational decisions regarding the satellites that it builds and controls. In NRO's view, others, principally its mission partners—NSA and NGA—which *are* designated as CSAs, are responsible for determining the requirements that guide NRO satellite designs and the operational tasking of deployed satellites. Now, however, there exists a class of operational decisions for which the NRO Director *is* responsible: in

situations in which U.S. satellites are under attack or threat of same, the NRO Director has the authority to make operational decisions regarding space control.

122. If confirmed, how would you ensure that the NRO is sufficiently integrated with and responsive to the U.S. Space Force? To U.S. Space Command?

If confirmed, I will work to strengthen collaboration between NRO and U.S. Space Force and the US Space Command in both development and operations. I believe the addition of the Director of the NRO as a member of the Space Force Acquisition Council will improve collaboration in space system development. For operations, the National Space Defense Center (NSDC) is the central point of integration and unity of effort. Accordingly, I would work with U.S. Space Command to ensure NSDC has a unified structure that fully integrates DoD and IC space defense plans and capabilities.

123. Given that NRO would be required to respond operationally to active threats to reconnaissance satellites by adversaries in a conflict, should the Department consider designating NRO as a CSA?

No, I believe the NRO has a unique role which is different from that of any of the Combat Support Agencies. For operational decisions regarding space control, the NRO and US Space Command have established a unified defense concept of operations at the National Space Defense Center to ensure integrated operations in times of conflict. In my opinion, this agreement provides the necessary unity of effort without designating NRO as a Combat Support Agency. Additionally, the Combat Support Agencies (NGA and NSA) are the functional managers and develop the collection priorities for the NRO assets.

124. How is the NRO synchronizing its acquisition efforts with the DOD Space enterprise and architecture?

Space system development benefits from collaboration across agency boundaries and the effectiveness of those systems improves with better interagency integration. If confirmed, I will consider how OUSD(I&S) can expand collaboration opportunities as the Department and the Intelligence Community (IC) move forward to orchestrate the development and fielding of a future threat-driven National Defense Space Architecture.

<u>Congressional Oversight</u>

In order to exercise legislative and oversight responsibilities, it is important that this committee, its subcommittees, and other appropriate committees of Congress receive timely testimony, briefings, reports, records—including documents and electronic communications, and other information from the executive branch.

125. Do you agree, without qualification, if confirmed, and on request, to appear and testify before this committee, its subcommittees, and other appropriate committees of Congress? Please answer with a simple yes or no.

Yes

126. Do you agree, without qualification, if confirmed, to provide this committee, its subcommittees, other appropriate committees of Congress, and their respective staffs such witnesses and briefers, briefings, reports, records—including documents and electronic communications, and other information, as may be requested of you, and to do so in a timely manner? Please answer with a simple yes or no.

Yes

127. Do you agree, without qualification, if confirmed, to consult with this committee, its subcommittees, other appropriate committees of Congress, and their respective staffs, regarding your basis for any delay or denial in providing testimony, briefings, reports, records—including documents and electronic communications, and other information requested of you? Please answer with a simple yes or no.

Yes

128. Do you agree, without qualification, if confirmed, to keep this committee, its subcommittees, other appropriate committees of Congress, and their respective staffs apprised of new information that materially impacts the accuracy of testimony, briefings, reports, records—including documents and electronic communications, and other information you or your organization previously provided? Please answer with a simple yes or no.

Yes

129. Do you agree, without qualification, if confirmed, and on request, to provide this committee and its subcommittees with records and other information within their oversight jurisdiction, even absent a formal Committee request? Please answer with a simple yes or no.

Yes

130. Do you agree, without qualification, if confirmed, to respond timely to letters to, and/or inquiries and other requests of you or your organization from individual Senators who are members of this committee? Please answer with a simple yes or no.

Yes

131. Do you agree, without qualification, if confirmed, to ensure that you and other members of your organization protect from retaliation any military member, federal employee, or contractor employee who testifies before, or communicates

with this committee, its subcommittees, and any other appropriate committee of Congress? Please answer with a simple yes or no.

Yes