Senate Armed Services Committee
Advance Policy Questions for Ms. Milancy Harris
Nominee to be Deputy Under Secretary of Defense for Intelligence and Security

Duties, Qualifications, and Relationships

1. **If confirmed as the Deputy Under Secretary of Defense for Intelligence and Security (DUSD(I&S)) what do you believe would be your most critical duties and responsibilities?**

   The Deputy Under Secretary of Defense for Intelligence and Security (DUSD(I&S)) is the first assistant to the Under Secretary of Defense for Intelligence and Security (USD(I&S)) and is responsible for assisting the Under Secretary in the performance of all of his or her duties.

   I understand that the responsibilities of the DUSD(I&S) are assigned in DoD Directive 5143.02. This directive provides that as the principal assistant to and under the authority, direction, and control of the USD(I&S), the DUSD(I&S) exercises full powers of the USD(I&S) on any and all matters on which the USD(I&S) is authorized to act, except in those areas where delegation of the USD(I&S) authority is otherwise restricted; helps the USD(I&S) carry out responsibilities, fulfill functions, manage relationships, and exercise authorities as provided for in law and DoDD 5143.01; and advises on and assists the USD(I&S) with all responsibilities in providing staff advice and assistance to the Secretary of Defense.

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

   My understanding is that the primary duty of the DUSD(I&S) is as the first assistant to the USD(I&S) and, therefore, the duties are similar. 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 pertaining to the National Intelligence Program (NIP), 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 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 DUSD(I&S), if confirmed?

I have had the privilege of serving in the Defense Intelligence Enterprise and the Intelligence Community for more than 15 years, including experience at the Defense Intelligence Agency, Office of Director of National Intelligence (ODNI), and on detail to the National Security Council (NSC) Staff. Additionally, I have experience in industry, managing governance and strategic intitiatives at Facebook and leading the establishment of the Oversight Board. I currently serve the Deputy Assistant Secretary of Defense for Irregular Warfare and Counterterrorism and have served in that position since February 2021.

These experiences have provided me with a broad appreciation for the responsibilities and contributions of our nation's intelligence professionals ranging from the foundational daily duties of our intelligence officers and briefers, the integration of multiple IC capabilities at ODNI, and the provision of intelligence support to our nation's most senior leaders. During my time in industry, I had the opportunity to experience different organizational management styles and varied approaches to levering emerging technology. In my current duties related to counterterrorism and irregular warfare, I have gained a deeper appreciation of the relationship between the IC and our warfighters.

If confirmed, I would use my experience to strengthen the development of our current and future generation of defense intelligence and security professionals within the broader IC and security communities to improve support to our warfighters. I would also pursue opportunities to rapidly and effectively leverage emerging technology for intelligence and security to enable our nation to stay ahead of its adversaries.

4. What is your experience across the domain of intelligence matters? What is your experience across the domain of security matters?

My career began with a series of foundational intelligence experiences and assignments, each preparing me for additional responsibility. I was initially trained as an intelligence analyst, focused on support to DoD acquisition decisions and then on analysis of global technology employment. I had the opportunity to serve as an executive intelligence briefer assigned to the Joint Staff, J2, and gained critical insight into the role intelligence plays in informing the Department's senior leaders. As I transitioned to counterterrorism, I had the opportunity to work in roles across the enterprise, including at the NSC Staff, where I gained valuable insights into warfighter requirements, policy maker needs, and operational analysis.

As a ODNI career officer, I also gained valuable experience working with the broader IC and understanding the domain of security matters. Given the unique role of the

National Counterterrorism Center (NCTC), I had an opportunity to work closely with law enforcement agencies and understand the U.S. Government's screening and vetting enterprise. While working as a Chief of Staff for NCTC's largest component, I gained an in-depth understanding of the personnel security role, including security clearances and IC reciprocity, as well as installation security.

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

   If confirmed, I would immediately begin to broaden my network and working relationships across the broader IC and security communities, including those within the ODNI, the other IC elements, and other defense elements and interagency partners within the security community.

6. **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), particularly with regard to oversight and management of the Defense Intelligence Agencies? 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 ODNI. The partnership and integration between OUSD(I&S) and ODNI enables the IC 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. Additionally, 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.

   If confirmed, I expect to assist the USD(I&S) in fulfilling these responsibilities through collaboration with my counterparts within ODNI and the Defense Intelligence Community elements.

7. **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?**

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

8. In your understanding, 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))?

My experience and understanding is that Office of the USD(I&S) (OUSD(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 U.S. Special Operations Forces (USSOF) intelligence and intelligence-related activities and programs. If confirmed, I look forward to continuing this close partnership, working with ASD(SO/LIC) to ensure that our oversight of USSOF intelligence and intelligence-related activities and programs is coordinated and collaborative.

9. 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 OUSD(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.

10. 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 cyber 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.

11. 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 OUSD(I&S) establishes policy for the Defense Civilian Intelligence Personnel System in partnership with the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD(P&R)). I also understand that OUSD(P&R) coordinates with OUSD(I&S) and the IC to identify and prioritize DoD foreign language capability requirements. If confirmed, I will examine the relationship between OUSD(I&S) and OUSD(P&R) to include the process for identifying DoD language capability requirements.

12. 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 understand 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 DoD intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters. The Directors for Defense Intelligence within the 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).

13. 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 (NDS). 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).

14. 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 OUSD(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 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 IC. 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.

15. 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 OUSD(I&S)?

I am committed to assist the USD(I&S) and 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 discuss the Department's defense intelligence, counterintelligence, security, sensitive activities, and other intelligence-related activities.

16. 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 assist the USD(I&S) fulfill his 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

DNI and the Director of the Federal Bureau of Investigation (FBI), 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

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

I consider supporting the NDS our most important responsibility. I anticipate strategic competition with China, deterring Russian aggression, and managing other persistant threats, including those from North Korea, Iran, and violent extremist organizations will be the most significant challenges. The Defense Intelligence and Security Enterprises have key responsibilities critical to the accomplishment of the 2022 NDS. They are responsible for providing intelligence that enables decision advantage for U.S. warfighters, decision makers, and Allies and partners. The Defense Security Enterprise must also safeguard personnel, information, operations, resources, technologies, and facilities against a wide range of threats and challenges.

If confirmed, I look forward to ensuring the Defense Intelligence and Security Enterprises further strengthen and provide the capabilities necessary to defend the homeland, deter strategic attacks, deter aggression and prepare for conflict when necessary, and support building a resilient Joint Force and defense ecosystem.

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.

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

Intelligence and security are mutually-reinforcing mission areas supporting NDS objectives. The Department must understand the intentions, capabilities, and activities of strategic competitors and other adversaries. Similarly, the security apparatus must safeguard our personnel, information, capabilities, and infrastructures, both physical and logical. The combination of these disciplines enables DoD's contributions to the United States' enduring advantage.

19. 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?

In my view, the Defense Intelligence and Security Enterprises represent a unity of effort, as they are mutually reinforcing mission areas. From my current vantage point, I believe the USD(I&S) has the authority and organizational structure to conduct appropriate oversight. If confirmed, I look forward to reviewing the resources of OUSD(I&S) and working with the Under Secretary to ensure that the resources and authorities necessary for oversight are available.

2022 National Defense Strategy (NDS)

In March, the Department of Defense transmitted to Congress the classified 2022 National Defense Strategy (NDS) and indicated that an unclassified NDS would be forthcoming. The 2022 NDS designates China as the pacing challenge for the United States, but it also states that Russia remains an acute threat to U.S. national interests. In addition, the Department must also manage the persistent threats posed by rogue regimes and violent extremist organizations.

20. In your view, how does the Office of the DUSD(I&S) directly support the NDS?

I believe the Defense Intelligence and Security Enterprises are critical to supporting the NDS. They are responsible for providing intelligence that enables decision advantage for U.S. warfighters, decision makers, and Allies and partners, while supporting integrated deterrence in support of NDS priorities. They are also responsible to safeguard personnel, information, operations, resources, technologies, and facilities against a wide range of threats and challenges.

If confirmed, as the first assistant to USD(I&S), I will work to ensure OUSD(I&S) efforts align to support the NDS and are resourced appropriately.

21. In your view, how would you assess the current readiness and capabilities of the Defense Intelligence and Security Enterprise to execute the NDS?

It is my understanding that the Defense Intelligence and Security Enterprises are well-postured to support the Department's execution of the NDS and are ensuring the proper alignment and allocation of resources.

If confirmed, I will prioritize developing my own assessment of the enterprises' readiness and capabilities to execute the NDS and working with the USD(I&S) to ensure the enterprises remain well-postured.

22. What do you believe are the main resource or capability shortfalls, if any, 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 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 OUSD(I&S) staff to identify promptly any obstacles likely to hamper execution of the NDS.

23. 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 (PPBE) process.

Strengthening Alliances and Attracting New Partners

Mutually beneficial alliances and partnerships are crucial to U.S. success in competition and conflict against a great power.

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

If confirmed, I commit to strengthening defense intelligence and counterintelligence relationships with allies and partners on issues of mutual concern such as Russian and Chinese malign activities, including ensuring we have the intelligence sharing relationships needed and the technology in place to facilitate sharing. The unique access and expertise of our Allies and partners enable us to close intelligence gaps and improve our mutual understanding of security issues that we face.

25. If confirmed, what factors would you consider in recommending 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 the factors that must be considered for foreign disclosure and release of U.S. classified military information, to include military intelligence, are stipulated in the National Disclosure Policy. If confirmed, I would support combatant command requirements for intelligence support to counter foreign malign activities and responsible foreign disclosure of military intelligence to friendly foreign governments and international organizations.

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.

26. 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 Joint Requirements Oversight Council (JROC) and Joint Capabilities Integration and Development System (JCIDS) processes use threat assessments from the IC to inform Joint Force capability requirements and to guide requirements and capability development, including in the areas of military intelligence, counterintelligence, and security.

As a statutory advisor to the JROC and its subordinate boards, USD(I&S) 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.

27. 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), to include for intelligence capabilities, from USD(A&S) to the Services. For example, the U.S. Air Force is now the MDA for the MIP-funded Next Generation Overhead Persistent Infrared satellites to provide missile warning.

However, changes to MDA have not altered how DoD addresses requirements or changed the JCIDS or JROC processes. The JROC continues its oversight of the JCIDS process and the assessment and validation of effective joint performance requirements in the areas of military intelligence, counterintelligence, and security. Additionally, an Intelligence Support Certification is still 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.

Successive Vice Chairmen of the Joint Chiefs of Staff have 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.

28. 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.

29. If confirmed, how would you ensure that NRO's responsiveness to JROC requirements 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 JCIDS and the Intelligence Community Capability Requirements (ICCR) processes.

If confirmed, I will work to maintain open communication throughout this process, and work closely with the Joint Staff and IC during the requirements validation process for National Reconnaissance Office (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.

30. What is your opinion of the effects of efforts to use Section 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.

If confirmed, I look forward to further reviewing the application of Section 804 to understand its applicability to, and value for, intelligence, counterintelligence, or security-related acquisitions.

Intelligence Support to the Warfighter

31. 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?

Balancing the intelligence needs of the warfighter and policy makers is one of the primary responsibilities of the OUSD(I&S). If confirmed, I will work with Department and IC stakeholders to ensure the Defense Intelligence Enterprise continues to satisfy all intelligence requirements for both our warfighters and senior policy makers in order to support decision-making by our national leaders.

32. In your view, what opportunities exist across the Intelligence Community to improve intelligence support to the warfighter, particularly in executing time-critical and complex kill chains? If confirmed, what would you do to leverage these opportunities?

I believe it is important to work across the Department and IC to find opportunities to improve support to the warfighter, including exploring technological innovations and process improvements.

If confirmed, I would engage with the combatant commanders to improve my understanding of their requirements and challenges. I would also frequently engage leaders within the IC and across the Department to ensure I understand current efforts to improve intelligence support to the warfighter.

33. In your view, are the Defense intelligence agencies, Joint Intelligence Operations Centers and Service Intelligence Centers organized and resourced to most effectively support warfighter requirements under the new 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?

In today's threat environment, most issues are relevant to both warfighting commands and policy makers, with targeting support tactically and operationally arrayed across the Services and Agencies. If confirmed, I will work to ensure the DIE continues to

satisfy requirements for operationally-relevant intelligence that directly enables warfighter success.

If confirmed, I will also support periodic reviews and realignment efforts to ensure priorities are met and resources effectively used to support the warfighter. I understand that the Joint Intelligence Operations Centers (JIOCs) have undergone various personnel reviews to determine the appropriate personnel levels to effectively support the mission requirements of the Combatant Commands. If confirmed, I will evaluate how to best resource the competing requirements of the Combatant Command JIOCs and the Service Intelligence Centers (SIC) to support the NDS. I believe that balancing the Combatant Command needs along with SIC requirements will be one of my primary responsibilities.

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

I am fortunate to be able to leverage the experience in my current role as the Deputy Assistant Secretary of Defense for Irregular Warfare and Counterterrorism where I work closely in this mission area with OUSD(I&S).

Intelligence operations executed by U.S. special operations forces (USSOF) are tactical operations in support of Combatant Commanders military objectives. The range of missions carried out by USSOF are unique because they executed on rapid timelines and in high-risk environments. USSOF missions require accurate, detailed, and timely intelligence that only integrated, multi-disciplined collection and analysis can provide. This tactical intelligence enables a commander to make rapid decisions while in contact with or close to the enemy. It is collected, analyzed, and quickly disseminated to the force enabling an integration of intelligence and operations that reducing risk to force and often creates opportunities for further collection and exploitation. Neither the capability nor the capacity is readily available within the IC or within conventional forces at the speed and scale required.

Other defense intelligence operations typically serve a more strategic purpose and generally focus on national intelligence requirements as part of the IC. While USSOF generally conduct intelligence to meet their own unique tactical intelligence requirements in support of the Combatant Commands, they are aware of and leverage intelligence derived from national collection priorities.

If confirmed, I will seek to leverage opportunities where intelligence operations carried out by USSOF will benefit the IC and vice versa.

35. 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?

In my current position, I am responsible for ensuring USSOF intelligence activities are closely coordinated with the IC as directed in applicable law, policy, and agreements. When USSOF engage in intelligence, counterintelligence, security, sensitive activities or other intelligence-related activities, the USD(I&S) and ASD(SO/LIC) share responsibility for overseeing those activities. If confirmed, I will continue to work closely with the ASD(SO/LIC), the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)), other DoD senior intelligence officials, and the IC to ensure USSOF comply with all applicable policies and directives to ensure Department oversight and coordination of USSOF activities and programs.

I believe that it is essential that DoD and the IC closely coordinate their activities, their training, the capabilities, and all aspects of their operations to ensure that, together, we achieve greater effects in protecting the United States. Additionally, I look forward to continued dialogue with the Committee to ensure clear and consistent reporting to the congressional oversight committees of intelligence activities carried out by USSOF.

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.

36. What is your understanding of the OUSD(I&S) participation in the JADC2 cross-functional team led by the Joint Staff J6?

It is my understanding that the OUSD(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 work closely within OUSD(I&S), with other DoD components, and with ODNI to make necessary improvements to the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) architecture to increase timely support to decision making at the strategic and operational levels.

37. 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, including by participating in experiments and exercises?

Yes, if confirmed, I will work closely with the USD(I&S) to appropriately apply his delegated authorities to shape required improvements to the C4ISR architecture to increase timely support to decision making at the strategic and operational levels in support of the Department's JADC2 initiative.

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.

38. 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?

Yes. Artificial Intelligence (AI) is critical for national and economic security. I concur with the NSCAI's conclusion that we must win the AI competition.

With the continued increase in the amount of information available both from traditional and open sources, the way to achieve a strategic advantage and ensure U.S. military and information dominance in competition and conflict is to develop and deploy world-class AI technologies. OUSD(I&S) has many strategic AI investments and partnerships that I understand will expand in the coming years, and if confirmed, I will assign the highest priority to the development and implementation of these capabilities.

39. Do you agree that the Defense intelligence components should take maximum advantage of the foundational AI platforms and tools that the Chief Data and Artificial Intelligence Office (CDAO) is sponsoring to develop AI applications for intelligence?

Yes. Defense intelligence components should take maximum advantage of the foundational AI platforms, tools, and investments that the CDAO sponsors.

If confirmed, I will work closely with the CDAO leadership to ensure these investments are leveraged to maximum effect and benefit for the Defense Intelligence Enterprise. I see the relationship between the OUSD(I&S) and CDAO as essential to maintaining our strategic advantage over our adversaries.

40. If confirmed, what actions would you take to support this effort?

If confirmed, I would advocate for the development of a robust partnership that fully integrates defense intelligence into the capabilities and platforms produced by the CDAO. For the CDAO to accomplish its mission, it must have access to data from the Defense Intelligence Enterprise.

41. Do you agree that the CDAO has oversight and supervisory authority over the Defense intelligence enterprise, including the intelligence agencies, with respect to data management and artificial intelligence?

CDAO is responsible for accelerating DoD's adoption of data and AI-enabled capabilities. They collaborate closely with Defense Intellignece Enterprise leaders to identify and remove barriers to effective data management and support the scaling of secure, responsible AI across our community.

42. 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?

I understand there have been several efforts instituted by the Department that have achieved great success over the last five years. These activities have spanned from fundamental research to the rapid fielding of technologies, demonstrating both the current and future potential of AI against the challenges we collectively face.

While the Department can be justifiably proud of these efforts, I believe that in order to meet future threats these capabilities must be scaled and refined. If confirmed, I would work with stakeholders across the Department to continue to pursue the application of AI capabilities to meet a variety of operational challenges.

Counterintelligence, Law Enforcement, and Security

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

DoD faces unprecedented foreign intelligence threats, principally from China and Russia. These threats target our personnel, capabilities, and infrastructure, across both the cyber and physical domains.

Our adversaries operate asymmetrically below the level of armed conflict using coercion, subversion, malign influence, disinformation, cyber and economic espionage, and spies and non-traditional collectors. In my opinion, the most concerning are those threats which aim to erode our warfighting advantage through targeting and exploitation of the industrial base.

44. 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) and recently released the first DoD CI Strategy in more than a decade, "Confronting Threats to America's Military Advantage, 2021-2031."

I also understand the USD(I&S) is a standing member of the National CI and Security Center's National CI Policy Board along with the Director of the Defense Intelligence Agency, as the statutory Defense CI Manager. Through this and other forums, the USD(I&S) coordinates and collaborates DoD CI activities across the U.S. Government.

If confirmed, I will work with USD(I&S) to provide strategic direction and leverage the Defense CI Manager and other critical leaders across the CI enterprise to ensure national priorities are addressed and the community continues to evolve to meet the future needs of the Department in this dynamic environment.

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

In my view, intelligence, counterintelligence, law enforcement, and security are mutually-reinforcing functions. As we face complex security challenges, DoD must integrate policy oversight of intelligence, counterintelligence, and law enforcement, along with foundational security functions, to enable the Department to better leverage a wide variety of tools to protect our people, information, and resources in support of NDS objectives.

Our intelligence professionals and special agents 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.

If confirmed, I will ensure that all communities under the authority, direction, and control of the Under Secretary continue to integrate and deny our adversaries freedom of maneuver.

46. 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? I do not believe the integration of these functions raises civil liberties concerns.

In my view, integrating these functions under one Principal Staff Assistant enables the alignment of policy, strategy, and resource prioritization by providing Department-level oversight of these disciplines.

It is my understanding that the OUSD(I&S) Counterintelligence, Law Enforcement and Security team are experts in the relevant authorities, privacy, civil liberties, and intelligence oversight laws and policies, reinforced by a strong legal team.

If confirmed, I commit to ensuring the continued integration of these complementary missions in a manner that respects civil liberties and protects any right or privilege secured by the Constitution or the laws of the United States.

47. 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 Counterintelligence, Law Enforcement, and Security portfolio within OUSD(I&S) has responsibility for the law enforcement policy function. Although I have not been fully briefed on current activities or resources, if confirmed I will review this portfolio and ensure OUSD(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.

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

Yes, I believe that DoD has benefitted from adopting the Interagency Security Committee's (ISC) security standards for DoD's leased commercial space.

In addition to reducing build-out costs and reconstruction times when DoD moves into a space previously occupied by another Federal tenant, aligning our standards for these spaces makes DoD a better, more-integrated co-tenant to 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 National Industrial Security programs. 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*.

In addition, 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.

Most of these very challenging new and enhanced requirements have been assigned to the Defense Counterintelligence and Security Agency (DCSA). A recent report on the DCSA's Industrial Security Program found that full implementation of these additional requirements would vastly increase DCSA's workload above current caseloads.

49. What is your current assessment of the ability of DCSA to transform itself to meet these objectives?

From what I have seen, the Defense Counterintelligence and Security Agency (DCSA) has done incredible work in reducing the investigation inventory and increasing its operational capability for detecting and mitigating insider threats. I recognize that DCSA must have the necessary support from OUSDI(I&S) leadership, as well as from the rest of the Deparment and interagency partners, to continue to meet its objectives.

If confirmed, I will be fully engaged with DCSA and the OUSD(I&S) staff to ensure the agency is appropriately positioned for continued success across all its missions.

50. Does DCSA currently have the budget and manpower to effectively execute these additional responsibilities?

DCSA is in a unique position where it is partially appropriated and partially operating under a fee-for-service model. As I understand it, DCSA is sufficiently resourced.

If confirmed, I would work closely with DCSA and appropriate stakeholders to ensure this model's continued success, but to also take a deep look into the appropriations to ensure the agency has what it needs to perform its critical mission.

51. 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 the DCSA recently issued its strategic plan, a first for the agency since the integration of missions from across the Defense enterprise and Office of Personnel Management. In issuing this plan, I understand DCSA extensively collaborated with its customers and external stakeholders to ensure it is meeting their needs.

If confirmed, I will work with DCSA leadership, as well as leadership across the Department, other executive branch agencies, and the Congress to support DCSA's implementation of its strategic plan.

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

If confirmed, understanding the consolidation and expansion of acquisition security missions at DCSA will be an area of significant focus for me.

Ensuring proper focus, partnership, and division of responsibilities across these functions is key to advancing acquisition security. I think an important step in the right direction, particularly in level-setting the expectations of the agency and its stakeholders, including OUSD(A&S) and the Military Departments, will be the review of the DCSA Charter.

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

As I understand it, Trusted Workforce 2.0 is a national-level effort, led by the DNI through the PAC, to reform personnel vetting across the Federal government. This effort aims to improve applicant engagement, effectiveness, and efficiency for personnel security, suitability, and credentialing. I believe the Department is deeply involved in this reform effort, as the USD(I&S) is a PAC Principal, and DCSA is the investigative service provider for much of the Federal government.

If confirmed, I will ensure the Department remains engaged and that DCSA is appropriately positioned for the success of this incredible reform effort.

54. 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 there is an important need to continually balance the tension between safeguarding classified information and assuring that same information is available,

when needed, for both government components and their contractors. This is particularly important for DoD, which I understand is the largest holder of classified national security information in the Federal government.

If confirmed, I look forward to supporting the review of information security processes and clearance reciprocity to meet the DoD's requirements to protect and appropriately share classified information.

55. 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 am aware that the Department is building a layered set of capabilities to detect and mitigate the Insider Threat. To be effective and efficient at the challenging mission of getting "left of crisis," I believe it is critical that the DoD Insider Threat enterprise—including the Defense Insider Threat Management and Analysis Center (DITMAC), Component Hubs, and installation-level insider threat personnel— have access to a wide range of data within the organization. This includes data from human resources, law enforcement, counterintelligence, personnel security, among others.

If confirmed, I would work to ensure a sustained effort is underway eliminate stove-piping and remove barriers to data sharing, as allowed by law.

56. In your view, how should insider threat architecture and activities overseen by OUSD(I&S) be integrated and coordinated with the Department's cybersecurity architecture and activities, especially with respect to the new emphasis on "zero trust" cybersecurity architectures and principles?

Success in areas of mission integration is founded in partnership. I am aware USD(I&S) and CIO have a strong working relationship and collaborate regularly on areas of mutual interest.

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 efficiencies across both missions of insider threat detection and cybersecurity.

57. Can zero trust practices, and network activity monitoring for cybersecurity, especially on DOD's unclassified network, promote, inform and augment insider threat detection? Can user activity monitoring for insider threat detection inform cybersecurity?

Yes. I understand Zero Trust assumes a network or system likely will be penetrated and builds internal cybersecurity controls to constrain malicious actors when they are

successful and alert DoD security and law enforcement when needed. Cybersecurity tools, network monitoring, and User Activity Monitoring (UAM) are valuable tools to augment other sources of data for identifying behaviors of concern early.

If confirmed, I will work to ensure policies and procedures are in place for UAM to be shared appropriately, including with cybersecurity elements as necessary.

58. In your view, should the Department's zero trust cybersecurity mandate and the CIO's role in supervising the implementation of zero trust apply to the Defense intelligence Agencies?

Yes. Zero Trust architecture benefits information systems security regardless of a system's functional purpose.

If confirmed, I will continue and grow OUSD(I&S)'s strategic partnership with DoD CIO and ODNI for IC systems regarding those operated by DoD IC Entities.

59. 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 the operational, technical, and acquisition programs, I believe the Department should maximize technology and the use of authorities to address the risk from the insider across all aspects of programs, including information sharing.

If confirmed, I will ensure the Department's insider threat efforts continue to integrate, innovate, and advance information sharing to enable a robust perspective of potential insider risk and/or threats.

60. 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?

The Department, as with all large institutions, faces common technical challenges when addressing large scale information technology systems that ingest, process, and store vast amounts of data. These challenges multiply as more users are involved and when the data is needed by multiple missions across different platforms. The protection of data and data sources are important considerations when addressing technical and system integration challenges.

If confirmed, I will work closely with the personnel security and insider threat communities to ensure information is shared, protected, and appropriately actioned.

61. 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 with DOD contractors' data systems? If so, how might such a program be implemented?

Although I have not been fully briefed on all the programs and constraints, the efficient and effective sharing of information between government and contractors is critical to detecting and mitigating the risk from insiders.

If confirmed, I will examine more closely the flow of information from contractor organizations in to the Department's Insider Threat Program, including DITMAC, and assess how the process and capabilities can be strengthened.

62. 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?

I have not been briefed on all aspects of these programs to assess if such a program is feasible or not. If confirmed, I commit to assessing all aspects of insider risk and ensure future goals and objectives include steps to ensure efficient and effective processes for passing information between contractors and the government.

63. 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 an effective Insider Threat programs is the support of the Component's leadership. This requires senior leaders to foster a positive workplace climate, encourage the reporting of concerning behaviors, and take seriously the responsibility for promoting awareness within the workforce. Additionally, senior leaders need to validate that their Insider Threat programs and other security functions, such as suitability and fitness determinations, credentialing, and vetting are meeting their requirements and are adequately resourced for success.

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.

64. 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?

I understand that after the December 2019 terrorist attack at Pensacola Naval Air Station DoD implemented new vetting policies for International Military Students

(IMS) and their accompanying family members that more closely aligned with the vetting DoD applies to U.S. military personnel.

If confirmed, I will work to continue to advance vetting policies and processes within DoD to provide a greater level of security for all personnel on DoD installations.

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 personnel and facility clearance processes and the hurdles that non-traditional contractors face in getting access to data to test and demonstrate new information technology and software.

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

I understand efforts are underway across the Defense Security Enterprise to meet the needs of the Department and keep pace with the speed of innovation today, with a particular focus on the clearance processes.

If confirmed, I would prioritize OUSD(I&S) security policy support to the acquisition and research and engineering communities as we seek to deliver uncompromised warfighting capability and enable the NDS.

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.

66. 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?

I would characterize the threat as significant and growing. The Department relies on U.S. innovation centers and academia, to undertake and advance science and technology that will maintain the lethality of the Joint Force and our allies. In my opinion, the most concerning are those threats which aim to erode our warfighting advantages through targeting and exploitation of the industrial base, particularly small businesses.

67. In your view, is the OUSD(I&S) and the DOD components it oversees 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?

I have not been fully briefed on the resourcing of OUSD(I&S) and the DoD components. However, if confirmed, I would recommend continued efforts to combat the misconception that security stifles innovation with rigid controls that deny scientist and engineers the ability to collaborate. Properly considered, properly applied, and continuously managed security practices are a critical, enabling element in research and innovation to encourage competition and protect DoD interests.

If confirmed, I would also support continuing initiatives to elevate, integrate, and optimize DoD security and counterintelligence to support and enable the security of the National Security Innovation Base.

68. 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 would support continuing initiatives, both within OUSD(I&S) and across the Department, to elevate, integrate, and optimize DoD security and counterintelligence to support and enable the security of the National Security Innovation Base. Key to this support is increased collaboration among the disciplines and across the interagency to ensure we are drawing on the vast capabilities of the National Security Innovation Base, including those with which would we not traditionally engage.

Classified Programs and Networks

The Deputy Secretary of Defense is leading a "zero-based review" of the status of special access programs (SAPs) to weed out activities that should not be handled in special access security channels and to enhance the protection of those that should remain SAPs. In addition, the Department is enhancing SAP management resources in order to cross-clear more personnel in industry and government to achieve more effective operational integration of SAP capabilities. The Department is also beginning to work on collapsing, integrating, and modernizing the SAP networks to achieve efficiencies in infrastructure and improve collaboration and integration.

69. In your view, how should the OUSD(I&S) be contributing to this effort?

I understand that OUSD(I&S) is fully supporting the Deputy Secretary's review. As the Department's Senior Agency Official for Security, and as one of four oversight

authorities for DoD Special Access Programs (SAP), the OUSD(I&S) is participating in the methodical and focused reviews of SAPs to ensure the information protected by these SAPs continues to be deserving of these exquisite protections. As determinations are made, if the information is deemed to no longer require SAP protections, OUSD(I&S) should aid in identifying and recommending other appropriate security protections.

Coming out of the review, OUSD(I&S) should continue to work with our IC partners to drive collaboration and integration of SAPs with other compartmented information, to include developing and leveraging common information technology systems to break down stovepipes and facilitate information sharing. Similarly, OUSD(I&S) should ensure that DoD SAP security policy allows for the appropriate enhanced security SAP information requires, while fostering integration and collaboration across government and with industry.

If confirmed, I would seek to ensure OUSD(I&S) continues to work collaboratively and effectively to support the Deputy's review and continued modernization of SAP networks and policies.

An expected benefit of accessing and cross-clearing more government and industry personnel managing and executing special access programs is the development of more effective "kill chains" and "effects chains" to support the Joint All-Domain Command and Control (JADC2) initiative. Intelligence support for this effort is critical. The JADC2 Implementation Plan issued by the Deputy Secretary of Defense calls for campaigns of experimentation and exercises to develop, test, and adopt novel kill chains.

70. If confirmed, how would you plan to ensure that the Defense intelligence components under the oversight and supervision of OUSD(I&S) prioritize support for this key warfighting and deterrence initiative to develop, experiment with, and exercise numerous and unexpected kill chains and effects chains?

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, which is 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 Department and IC stakeholders to shape required improvements to the C4ISR architecture to increase timely support to decision making at the strategic and operational levels.

Intelligence Oversight

71. 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.

72. 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 current process, in which the Principal Deputy Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency (PDATSD(PCLT))/Senior Intelligence Oversight Official notifies the President's Intelligence Oversight Board (PIOB) of Questionable Intelligence Activities and Significant or Highly Sensitive Matters, is effective.

If confirmed, I look forward to fostering a positive relationship between OUSD(I&S) and the PDATSD(PCLT)/Senior Intelligence Oversight Official in engaging the PIOB, ensuring that my office provides subject-matter expertise, as required by DoD policy, to support the PDATSD(PCLT)/Senior Intelligence Oversight Official 's inspection, investigative, and reporting activities, including its 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.

73. 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 and Security Enterprise must support the Department's efforts to compete in the information environment and gain or maintain a competitive advantage. My view is that the Department should conduct military operations in the information environment across multiple domains to counter foreign malign actors to advance U.S. national security interests.

Our efforts to deter and defend against foreign strategic information operations should be prioritized and must include robust coordination and collaboration across the Department, including with the USD(P) acting as the Secretary of Defense's Principal Information Operations Advisor, and the Executive Branch.

74. 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 OUSD(I&S) Task Force on Strategic Competition and Influence in your view?

In my current role, I understand the USD(P) is the Principal Staff Assistant for Information Operation (IO) and is currently working on a Congressionally mandated posture review and strategy for IO. The USD(I&S) has detailed personnel to support this effort since the USD(I&S) has responsibility for coordination of DoD IO activities within the IC, as well as the development and implementation of DoD policy, programs, and guidance for DoD deception, operations security, influence, and reveal/conceal activities.

I believe that USD(P) and USD(I&S) are important partners in the effort to position the Department for the challenges in today's information environment. If confirmed, I would seek to work with the USD(P), the Chairman of the Joint Chiefs of Staff, and other DoD leaders to ensure our collective organizational approach on Information Operations to optimized to achieve our national security goals while also meeting the most rigorous standards for oversight.

I understand Secretary Austin directed the USD(I&S) establish an Influence and Perception Management Office (IPMO). If confirmed, I will seek to understand the status of IPMO's establishment and how it is integrated with other elements across the Department.

75. What are your views regarding the designation of an Information Operations Joint Force Provider and Trainer, as mandated by Congress but which DOD has yet to implement?

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

76. 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 their ability to support combatant commanders by fully understanding the information environment and adversaries activities within; by engaging and potentially partnering with those who are impacted by foreign malign influence and coercive operations; and by enabling

efforts, in alignment with national and defense priorities, to attain and sustain competitive U.S. national security advantages.

77. 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 would make it a priority to attribute, expose, and counter foreign malign activities that harm U.S. national security interests.

Cyber Strategy

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. Currently, DOD is in the process of updating its cyber strategy.

78. 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 and the current updating of that Strategy?

My understanding is OUSD(I&S) has a developed a strategy for intelligence support to cyberspace operations. In addition, I understand that OUSD(I&S) is engaged with the Principal Cyber Advisor (PCA) and OUSD(P) on the update of the DoD Cyber Strategy.

If confirmed, I will commit to ensuring the Defense Intelligence Enterprise is well-postured to support the operationalization of the Department's Cyber Strategy.

79. 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 current and emerging Cyber Strategy?

If confirmed, I will commit to assessing the findings in the Cyber Strategy to include any gaps between the Defense Intelligence and Security Enterprise capacity and capability to support. If confirmed, I will ensure that OUSD(I&S) fully participates in efforts to address any of the potential gaps this future strategy may identify.

80. 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?

It is my understanding that Secretary Austin recognizes any decision on the Dual-Hat should be based on comprehensive analysis of the impact on both organizations'

effectiveness and he will work with the DNI as he assesses of the value and ongoing benefit of the Dual-Hat leadership arrangement.

I believe that any recommendation about the future of the dual-hat leadership arrangement must be based on a thorough understanding of the operating environment, the military and intelligence priorities, and the operational capability and capacity of both U.S. Cyber Command and the National Security Agency**.** If confirmed, I will seek to support the Secretary and USD(I&S) in conducting any assessments of the Dual-Hat leadership arrangement.

81. 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?

I understand that OUSD(I&S), in partnership with the PCA and the Chief Information Officer, is committed to the cybersecurity mission.

If confirmed, I will ensure that the OUSD(I&S) is well-postured to support the Department's efforts to safeguard vital information and technologies in DoD and in the Defense Industrial Base against evolving and increasingly sophisticated threats in and thorough cyberspace, including by ensuring adequate intelligence support to cyber activities.

Interrogation Techniques and Detainee Treatment

82. 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 March 15, 2022?

Yes. I believe these policies represent the values and behavior expected of our military members.

Imperative for Independent Intelligence Analysis

83. 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?

Independence and freedom from political bias are central to the profession of intelligence analysis. If confirmed, I would emphasize the importance of analytic integrity to all members of the Defense Intelligence Enterprise, no matter their assigned location, and work to ensure that they are free to conduct their work without political pressure or influence.

The Defense Civilian Intelligence Workforce

The OUSD(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.

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

I have not yet had an opportunity to analyze the defense civilian intelligence workforce in its size and capability, but I believe people are any organization's most important resource.

If confirmed, I will seek to ensure the Defense Intelligence Enterprise is appropriately resourced to provide timely and reasoned intelligence products to the warfighters and policy makers.

85. 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 the IC, and particularly my time at the Defense Intelligence 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 analyze our workforce alignment to the NDS and offer recommendations if needed.

86. 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 an organization's most important resource. If confirmed, I will work to ensure the workforce is comprised of the most qualified intelligence and security professionals, and that opportunities to expand candidate pools to acquire both the skills and diversity necessary to accomplish DoD intelligence and security missions are aggressively pursued.

87. 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 focus on identifying, selecting, and developing all personnel to accomplish our mission objectives, including DISES and DISL.

88. 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?

If confirmed, I will follow the USD(I&S)'s plan to continue using the executive performance management system to maintain oversight of executive and senior level performance.

89. What is your understanding of the subject matter and rigor of DISES and DISL professional development programs currently available across DOD? What changes, if any, would you make to these programs, if confirmed?

I have not yet been briefed on these professional development programs within the Department. However, if confirmed, I plan to understand these programs effectiveness as a talented and effective leadership cadre is critical to providing quality intelligence to the warfighter and policy maker.

90. What is your understanding of the effectiveness of the process employed by the OUSD(I&S) to validate whether a vacant DISES/DISL position should be rehired, restructured, or eliminated 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 validation process for DISES and DISL positions. However, I understand that continuous evaluation of requirements is essential to ensuring leadership positions are appropriately resourced and structured.

If confirmed, I will ensure the continued oversight of the processes 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.

91. 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?

Joint experience supports a fully integrated and collaborative IC. Similar to the way that the military joint duty requirements from the Goldwater-Nichols Act have paid dividends for the military services, the civilian joint duty program is vital to building a more integrated, interoperable, and effective IC.

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 IC and that throughout their careers they build deep and enduring professional relationships across the IC.

92. 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 within the DoD and the ODNI, 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 our most demanding technical areas, to ensure we have the expert, professional, and motivated workforce the 21st century demands.

If confirmed, I will ensure continued support for the IC's 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, and commit to engaging the Committee on our recommendations.

93. 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 support the USD(I&S)'s review of the authorities available to the Department and assess whether any additional authorities are required to address DCIPS challenges.

Unidentified Aerospace and Transmedium Phenomena

Congress has enacted legislation, provided direction, and authorized and appropriated funds for the Department of Defense and the Intelligence Community to increase the scope, focus, and resources devoted to identifying and understanding the many credible observations spanning years of unidentified objects in restricted military training areas and in areas where U.S. military forces are operating. These congressional actions and mandates go beyond the tasking by the Deputy Secretary for establishing a new task force under the USD(I&S).

94. What is your understanding of congressional mandates in this area?

I understand the congressional requirements for regular briefings and reports to members and staff, including continuing the DNI's annual unclassified report; the expansion of the scope to include airborne, submerged and transmedium objects; and the importance of coordinating DoD, IC, and U.S. government efforts in this area.

95. If confirmed, do you support fully executing the congressional mandates for addressing this problem set?

Yes. If confirmed, I will support fully executing the requirements established in statute, while ensuring the Department is properly postured to address the concerns and threats posed by anomalous unidentified objects in all domains.

96. How will you ensure that collection and analysis is not confined to just events occurring in restricted DOD training airspace and to objects observed in the atmosphere?

I believe it is critical that the Department works to detect, analyze, identify, and, if necessary, mitigate anomalous unidentified objects in all domains, including in space, air, and underwater, as well as transmedium objects.

If confirmed, I look forward to ensuring that the Department is adequately postured to address anomalous events regardless of the domain or area in which they occur.

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.

97. 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 will support USD(I&S)'s commitment in ensuring protections are afforded to Defense Intelligence and Security Enterprise 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.

98. 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 support USD(I&S)'s responsibilities in ensuring DoD policy implementing such protections is applied consistently and uniformly in accordance with law.

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.

99. 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 DoD and IC space organizations to enable collaborative work and the sharing of mutually-beneficial capabilities.

100. 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.

As there is growth in the collection and analytical needs of space intelligence and defense missions, it will be important to look for process improvements to streamline relevant processes. If confirmed, I will work with the Functional Managers on ways to increase access, agility, and responsiveness to best satisfy these unique space intelligence requirements.

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.

101. 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, U.S. Space Force, and U.S. Space Command in both development and operations.

I believe the addition of the Director of the NRO as a member of the Space Acquisition Council improves collaboration in space system development. The National Space Defense Center (NSDC) is the central point of integration and unity of effort for operations. Accordingly, if confirmed, I would work with U.S. Space Command to ensure NSDC has a structure that fully enables integrated DoD and IC space defense plans and capabilities.

102. 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 (CSA) in that NRO develops capabilities that fulfill requirements from the NSA and NGA as the Defense Intelligence Enterprise Managers (DIEMs) and IC Functional Managers.

For operational decisions regarding space control, the NRO and U.S. 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.

103. 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 IC move forward to orchestrate the development and fielding of a future threat-driven resilient National Defense Space Architecture.

Sexual Harassment

In responding to the 2018 DOD Civilian Employee Workplace and Gender Relations survey, approximately 17.7 percent of female and 5.8 percent of male DOD employees indicated that they had experienced sexual harassment and/or gender discrimination by "someone at work" in the 12 months prior to completing the survey.

104. What is your assessment of the current climate regarding sexual harassment and gender discrimination in the DOD?

As a member of the Department, I support the actions directed in the Secretary's February 2021 memo to senior DoD Leadership in countering sexual assault and harassment. With the Secretary's focus on this important issue, we as leaders must be held accountable in driving meaningful change and be part of the solution to improve

the climate allowing all members of the DoD to serve with dignity and respect.

105. 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 DoD or the IC. If confirmed, I will support the USD(I&S)'s 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.

Congressional Oversight

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.

106. 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.

107. 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.

108. 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.

109. 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.

110. 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.

111. 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.

112. 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.