Senate Armed Services Committee
Advance Policy Questions for Mr. Bradley Hansell
Nominee for Appointment to be
Deputy Under Secretary of Defense for Intelligence and Security

Duties, Qualifications, and Relationships

Section 137a of title 10, U.S. Code, establishes the position of the Deputy Under Secretary of Defense for Intelligence and Security (DUSD(I&S)) and provides that the DUSD "shall be appointed from among persons who have extensive experience in intelligence matters."

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

   If confirmed, I will assist the Under Secretary of Defense for Intelligence and Security (USD(I&S)) in support of the Defense Intelligence and Security Enterprise (DISE) as it works together to conduct intelligence activities in support of the national security of the United States. I will always focus on ensuring the warfighter and the policy maker are supported to that end.

   I believe the Intelligence Community (IC) must constantly strive to be an integrated, agile, and mission-driven intelligence enterprise that embraces innovation. The DISE must continue to be adaptive, diverse, continually learning, and mission-driven. I understand that critical duties and responsibilities of the DUSD(I&S) include ensuring intelligence support to Combatant Command (COCOM) and Departmental requirements, and the synchronization of military, defense and national intelligence capabilities.

2. **What is your understanding of the role of the DUSD(I&S) as "first assistant" to the Under Secretary of Defense for Intelligence and Security (USD(I&S))?**

   As the principal assistant to the Under Secretary, the DUSD(I&S) assists the USD(I&S) in carrying out the responsibilities, fulfill functions, manage relationships, and exercise authorities as provided for in law and DoD Directive 5143.01, including the exercise of authority, direction, and control on behalf of the Secretary of Defense over the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Security Agency/Central Security Service (NSA/CSS), the National Reconnaissance Office (NRO), and the Defense Counterintelligence and Security Agency (DCSA). In addition, the DUSD(I&S) assists the USD(I&S) in planning, policy, and strategic oversight for all defense intelligence, counterintelligence and security policy, plans, and programs. Lastly, the DUSD(I&S) advises on and assists the Under Secretary with all responsibilities in providing staff advice and assistance to the Secretary of Defense. If confirmed, as a leader in the Department it is an implied responsibility, when appropriate, beneficial, and lawful, to collaboratively support the intelligence-related needs for the whole-of-government mission to protect our nation's security.

3. What is your understanding of the differences between the title 10 and title 50 duties of the USD(I&S)—duties that, in regard to some matters, could be delegated to you if confirmed as the DUSD(I&S)?

My understanding is that the USD(I&S) assists the Secretary of Defense in satisfying all of the Secretary's 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 sections 137 and 137a of title 10 of the United States Code (U.S.C.), the DUSD(I&S) may exercise the full powers of the USD(I&S) on any and all matters on which the USD(I&S) is authorized to act, as delegated by the Secretary of Defense in DoDD 5143.01, except in those areas where delegation of the USD(I&S) authority is otherwise restricted by higher authority or prohibited by law.

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

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

I am passionate about helping people and organizations realize their highest potential. Throughout my career, I have sought opportunities to be a student and a practitioner of leadership to enable that objective. If confirmed, I look forward to bringing my experience forward to be an effective servant leader within the Department of Defense and DISE. I believe my experience in the United States Navy, the United States Army Special Forces, and the National Security Council, coupled with my work in the commercial sector doing both commercial and public sector consulting have uniquely prepared me for this position.

After college, I initially chose to join the Navy's Surface Warfare Community, inspired by the responsibility of leadership and opportunity to serve our nation. My early tours as a Naval Officer taught me many lessons about how to get things done in a large, matrixed enterprise. Seeking more impact, I entered Naval Special Warfare Training, which provided the foundation for the character and leadership principles I bring forward today. After leading my class through 'hell week' and a medical disqualification later in training, a transfer to the Army Special Forces provided the experiences that would

deepen my commitment to these principles. I am honored that some of these experiences included leading America's finest in combat. These responsibilities prepared me to be a strong manager able to generate a vision, build consensus, and drive execution. Most importantly, my experiences have ingrained in me the value of servant leadership.

After my retirement from the military, I attended graduate school for an MBA to learn how to best apply these leadership lessons in the business world. I have twice worked at Boston Consulting Group, a management consulting firm that advises the world's largest organizations on how to address some of their most challenging leadership and management challenges. This experience furthered my ability to be a strategic thinker, capable of challenging the status quo, in search of innovative solutions. As a leader in the North American Public Sector practice and as a Senior Director at the National Security Council, I understand the unique leadership and managerial challenges facing our government today.

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

As a Senior Director on the National Security Council staff, I helped lead efforts in furtherance of a directorate focused on transnational threats. Part of my mandate was to identify and seek to eliminate any bureacratic silos that limited our collective capacity in areas of my portfolio. I believe this integration is critical in both policy and organizational design in order to address all of our adversaries‘ sources and strength and support, including in a key area of focus at the time for the Administration, transnational organized crime (TOC).

On February 9, 2017, President Trump issued Executive Order (EO) 13773, which, *inter alia*, called for enhanced efforts to "maximize the extent to which all Federal agencies share information and coordinate with Federal law enforcement agencies, as permitted by law, in order to identify, interdict, and dismantle transnational criminal organizations and subsidiary organizations." The first interagency report in response to EO 13773 confirmed that the Federal government did not have the requisite structures in place to adequetely coordinate activity and also lacked the capability to provide a comprehensive picture of the threat environment.

Recognizing the importance of establishing an interagency framework that can both map and action the threat enviroment, my team began to build consensus for a permanent integrated effort to meet the intent similar to what National Counterterrorism Threat Center (NCTC) does for intergrating CT intelligence and planning. Our effort sought to develop the basis for increased data integration and a national level planning process. In the process of standing up a new coordination mechanism, we encountered many of the barriers that had hardened bureaucratic silos in the past – such as competing policy priorities, legal authorities issues, and widely differing but well-established mindsets that fostered organizational resistance to change.

Despite all of these obstacles, we successfully navigated a path to consensus to establish a new whole-of-government framework for tackling TOC. These efforts yielded, *inter alia*, better integration with the Department of Treasury and the Department of Defense and a new interagency planning capability located at the Department of Justice National Terrorist Screening Center. Today, these additional capabilities and increased coordination among Federal agencies have established an integrated policy planning process with a permanent focus on improving the integration of available investigative, regulatory, and law enforcement information required to address TOC in a more holistic and comprehensive way.

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

My career as a national security professional, spanning nearly twenty years, has provided me significant experience in intelligence and security matters, from the tactical to the national level.

As an Army Special Forces Officer, my team and I were both consumers and collectors of intelligence. I experienced firsthand its impact on informing the fidelity of strategy and operations. I personally leveraged intelligence in my management of risk to force when leading men in combat.

Serving as a Senior Director in the National Security Council, I saw the criticality of timely and accurate intelligence to inform policy makers. As part of my responsibility, I worked to ensure strategy was informed by adequate and coordinated intelligence collection. This experience afforded me the opportunity to become familiar with intelligence processes at the national level.

Leading a functional directorate on the National Security Council gave me exposure to threats and policies globally and the intelligence and security issues that supported them. In my responsibility to align inter-agency policies and resources to a national problem set, part of my role within my portfolio included working with elements of the Intelligence Community to better integrate toward a unified objective. If confirmed, this experience would inform my view on the criticality of integration across our intelligence components and enhances my ability to be a valuable stakeholder in its execution.

7. 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, leveraging the experience and wisdom of the career professionals within the DISE and throughout the Department will be critical to my own and the organization's success. I believe in the value of seeking knowledge in every direction and will do so if confirmed. Furthermore, I would work to ensure an organization climate that encourages the best ideas to flow freely through the organization.

From my understanding of the responsibilities of the OUSD(I&S) and requirements in support of DoD, the broader IC, and the whole of government, it is imperative to foster and facilitate a collaborative environment to achieve mission success. If confirmed, I will personally work to maintain strong relationships and seek new opportunities for collaboration with stakeholders.

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

In my preliminary conversations with the USD(I&S), I have learned of the Secretary's increasing focus on posturing the DISE against the threats posed by great power competition, specifically against China and Russia. If confirmed, I anticipate that in addition to assisting the USD(I&S) in his authority, direction, and control of the DISE, I will help OUSD(I&S) accomplish the goals the Secretary has set for the DISE in posturing against China and Russia.

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

As a proud veteran, I fully support the fundamental requirement for civilian control of the Armed Forces. The partnership of the civilian, military, and contractor team in the Department is essential to accomplishing our national security objectives. Yet, ultimately, adherence to the principle of civilian control of the military ensures that our military is ultimately responsive to our Nation's elected representatives, and by extension, the American people that they protect.

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

The OUSD(I&S) works closely with the Office of the Director of National Intelligence (ODNI) to effectively integrate intelligence in support of U.S. national security interests. Through the effective partnership and integration between OUSD(I&S) and ODNI, the Intelligence Community delivers coordinated intelligence to policymakers and warfighters on crucial threats to our national security.

The USD(I&S) himself is dual-hatted as the Director of Defense Intelligence at ODNI and there is a military officer who serves as the DNI's Advisor on Military Affairs (DAMA) to ensure tight coordination between the Department of Defense Intelligence Enterprise (DIE) and the greater IC. The staffs must coordinate to effectively and efficiently ensure quality intelligence is provided in support of our national leadership

and Warfighters. I believe that USD(I&S) plays a critical role and is effective in ensuring IC support to Warfighters.

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

My understanding of DoD Policy is that the Under Secretary of Defense for Policy (USD(P)) is the Principal Staff Assistant (PSA) for information operations and that this responsibility is executed through the Information Operations Executive Steering Group (IO-ESG). My understanding of DoD policy is that the USD(I&S) has responsibility for coordination of IO activities within the Intelligence Community as well as the development and implementation of DoD policy, programs, and guidance for DoD Deception and operations security (OPSEC).

More importantly, I consider influence and counter-malign influence critical DoD activities that enhance the U.S. Government's ability to strategically compete against the National Defense Strategy (NDS) threats. If confirmed, I will continue to foster a close and effective working relationship between the USD(P) and USD(I&S) for related Information Operations Activities and will continue to support the Secretary of Defense's emphasis on these activities**.**

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

I understand that the USD(I&S) is responsible for supporting the Secretary of Defense in discharging his intelligence and security responsibilities and authorities under Title 10 and Title 50 of the United States Code. This includes exercising authority, direction, and control on behalf of the Secretary of Defense over certain defense intelligence components of the Department of Defense and working closely with the Joint Staff, Combatant Commands, Service Components, and the ODNI to develop effective policy, plans, programs, and priorities. The optimal relationship between OUSD(I&S) and the Chairman of the Joint Chiefs of Staff is mutual support and consultation to ensure the defense intelligence enterprise (DIE) provides the warfighters with the best intelligence possible, to conduct their planning and operations and to provide the Secretary of Defense with the best defense intelligence and military advice.

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

I understand that USD(I&S), the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD(SO/LIC)) and the Department of Defense Senior Intelligence Oversight Official (DOD SIOO) are the primary oversight officials for all

Special Operations Forces (SOF) intelligence and intelligence-related activities and programs.

I believe strengthened coordination among and between these offices helps to ensure that the United States is best postured to maximize our effects. If confirmed, I will work to ensure defense intelligence activities adhere to appropriate coordination processes with the Office of the Secretary of Defense.

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

Currently, I am not aware of any issues. However, I would need to better understand the full range of program oversight. If confirmed, I would work closely with ASD SO/LIC and the Commander of U.S. Special Operations Command (USSOCOM) to help ensure that supporting activities and programs are in place and overseen to support USSOCOM and are aligned appropriately to ASD(SO/LIC)'s roles and responsibilities.

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

I understand the relationship between OUSD(I&S) and the Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSD(A&S)) is one of cooperation and collaboration; however, I do not have the insight necessary to provide a fulsome assessment of how they divide their responsibilities across a very large DISE portfolio. If confirmed, I will learn more details of their relationship, and where I see challenges, I will provide my recommendations to the USD(I&S) on how best to address those concerns.

Within the context of both strategic competition and the technology environment in which it will occur, I believe the criticality of informing our acquisitions and investments with the best possible intelligence is at an all time high and will continue to increase. Furthermore, in light of the growing loss of our technological edge to theft and compromise, it is essential to consider security throughout the acquisition process, a factor on an equal footing with cost, schedule, and performance in the success of our defense acquisitions. If confirmed, I will work toward continuing the cooperation and collaboration of these offices to support this end.

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

The relationship between the OUSD(I&S) and the Department of Defense Chief Information Officer (DoD CIO) must be based on collaboration and partnership to ensure synchronization between security policy makers and IT service providers. The magnitude of data to be leveraged and the proliferation of wireless devices, Internet of Things, and the threats they pose to information security, underscore the importance of this effort. Success depends on teamwork. 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 on the operation and protection of all DoD information technology and information systems. If confirmed, I will ensure OUSD(I&S) maintains a close partnership with the DoD CIO to enable the necessary security architecture to protect intelligence and counterintelligence information while effectively enabling the mission.

17. How do you view the relationship and division of responsibilities between the OUSD(I&S) and the Commander, U.S. Strategic Command, with regard to the Battlespace Awareness Capability Portfolio?

I understand that under DoD Directive 7045.20, Capability Portfolio Management (CPM) for the Battlespace Awareness Portfolio, the USD(I&S) is the designated civilian lead and United States Strategic Command (USSTRATCOM) is the military lead. The USD(I&S) assesses BA capability requirements, current/future programs and Service/Combat Support Agency BA programming and budgets. USSTRATCOM provides inputs on requirements to the Joint Staff for its annual capability gap assessment. Additionally, both USSTRATCOM and OUSD(I&S) participate in the Department's annual program review providing recommendations to leadership on portfolio investments.

18. 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?

I have not been fully briefed on the relationships and divisions of responsibilities between OUSD(I&S) and the USD(P&R). However, it is my understanding that the USD(I&S) develops the policies for the Defense Civilian Intelligence Personnel System (DCIPS) in close coordination with the USD(P&R).

The relationship between the USD(I&S) and the Under Secretary of Defense for Personnel & Readiness (USD(P&R)) has worked similarly with regard to the foreign language programs. However, I understand that as part of the Defense Wide Review the intelligence language programs are slated to transfer in fall 2020 from OUSD(I&S) to OUSD(P&R) to be integrated with the Department's larger foreign language office, the Defense Language and National Security Education Office (DLNSEO). At this time, I believe that integration of these programs could result in more efficient operation; however, if confirmed, I will review and lend my advice on the matter as appropriate.

19. How would you order the relationship between the OUSD(I&S) and the heads of the Intelligence Components of the Military Departments? What factors would you recommend that the USD(I&S) consider and weigh in providing input to the Secretaries of the Military Departments on the duty performance of the heads of their respective Intelligence Components?

I believe that the OUSD(I&S) staff has a deep relationship with the heads of all of the Service intelligence components and Combat Support Agencies. The USD(I&S) established the Defense Intelligence and Security Integration Council (DISIC) to bring the leaders of the Defense Intelligence Enterprise (DIE) together regularly to discuss and address key issues. I believe it would be appropriate for the USD(I&S) to weigh collaboration, innovation, and NDS implementation heavily when providing input to the Secretaries of the Military Departments on the duty performance of the heads of their respective intelligence components.

20. 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.

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

As the MIP Executive Agent, the USD(I&S) has management and oversight of the Military Intelligence Program (MIP). The USD(I&S), in the roles of the Director of Defense Intelligence and has visibility into the NIP through participation in ODNI resource decision forums. Additionally, I understand that the DNI and the USD(I&S) jointly sign out intelligence programming guidance to closely synchronize NIP and MIP programs to ensure that the Department's priorities are communicated to the intelligence community. If confirmed, I will work closely with the Office of the Director of National Intelligence (ODNI) in ensuring that the Department's 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; therefore, there is little, if any, substantive difference.

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

I am committed to assist the Secretary of Defense in fulfilling his obligations to congressional oversight. Specifically, regarding the Senate Armed Services and Senate Appropriations Committees, if confirmed, I look forward to engaging with the committees to communicate the Department's budgets and activities.

23. 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 assisting the USD(I&S) in fulfilling 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 Director of National Intelligence and the Director of the Federal Bureau of Investigation, as appropriate, and notify Congress, as required by section 2723. If confirmed, I will examine how the OUSD(I&S) supports the USD(I&S) with respect to this responsibility and pursue improvements, as needed, to ensure such notifications are accurate, complete, and timely.

Major Challenges and Priorities

24. What do you consider to be the most significant challenges you would face if confirmed as the DUSD(I&S)?

Based on my understanding of the National Defense Strategy and current OUSD(I&S) priorities, I believe that the intelligence activities required to ensure we are most able to effectively inform our acquisitions and investments, support full spectrum operations, and maximize the advantage of our national security innovation base will remain significant challenges.

To ensure the Department is best postured to retain advantage in both competitive and contested environments, the foundational military intelligence necessary to inform great power competition and the technology environment in which that competition will occur is critical. The technology environment has the potential to fundamentally alter warfare and national security now more than any other time. With the cost of the programs required to mitigate the threat environment and to retain the military advantage incredibly high and the cost of misallocation even higher, the premium on intelligence informing our investments and acquisitions has never been more important. This year's Senate markup of the National Defense Authorization Act— containing the largest R&D budget in history— reflects the importance of having the best intelligence to inform DoD

investments and acquisitions.

As adversaries continue to increase their malign activity short of armed conflict, the ability of the Department to conduct effective full spectrum operations and coordinate broader whole of government activity will remain essential. Providing timely and accurate integrated intelligence that informs policy makers on new threats, such as Chinese espionage and Russian disinformation, its impact, and potential opportunities in this dynamic environment will remain a significant challenge.

Ensuring we are fully leveraging and protecting our national security innovation base will remain a significant challenge. Budgets and the threat environment will continue to reinforce the imperative of fully leveraging commercial technologies to build our intelligence and security capabilities. This may require innovative advances to our traditional investment and acquisition methodologies. Equally important, the required effort to ensure we are protecting against adversary exploitation of our innovation advantage will continue to rise and require coordination further into the defense innovation base.

25. If confirmed, specifically what actions would you take, in what order of priority, and on what timeline—to address each of these challenges?

I feel it is premature for me to detail a specific plan of action at this time before I have been briefed on the full suite of ongoing OUSD(I&S) activity, to include classified information and programs. However, if confirmed, I will rapidly assemble all relevant data and a complete picture of DoD capabilities to address the full spectrum of issues. In doing so, I will coordinate with USD(I&S), Department, and IC leaders, and seek input and guidance from this committee along with other committees of jurisdiction, to identify an informed set of prioritized actions and focus areas.

26. If confirmed, what innovative ideas would you consider providing the USD(I&S) regarding the organization and operations of the OUSD(I&S)?

I feel it is premature for me to propose organizational changes at this time, before I have been briefed on the full suite of ongoing OUSD(I&S) activity, including classified programs and information. However, if confirmed, I will rapidly assemble all relevant data and a complete picture of our capabilities to address the full spectrum of issues. In doing so, I will coordinate with USD(I&S), Department, and IC leaders, and seek input and guidance from this committee along with other committees of jurisdiction, to identify an informed view on areas that may most benefit from innovative ideas.

<u>Supervision, and Oversight of the Defense Intelligence and Security Enterprise</u>

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.

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

As Principal Staff Assistant (PSA) to the Secretary of Defense regarding intelligence, counterintelligence, security, sensitive activities, and other-intelligence related matters, the USD(I&S) exercises oversight over the DISE. OUSD(I&S) works across the Department with the Military Services and defense agencies to identify requirements and capabiltiies to meet DoD priorities. We work closely with the ODNI to ensure the national intelligence priorities take into account Departmental requirements. These efforts ensure Enterprise alignment with all national and Department-level strategies, guidance, direction, and relevant priorities. The USD(I&S) also executes the Military Intelligence Program (MIP) and participates in the ODNI specified National Intelligence Program (NIP) process to ensure resources are aligned against DoD priorities.

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

I believe that the USD(I&S) has sufficient authority to provide policy oversight of the DISE. If confirmed, I will work with OUSD(I&S) staff to determine if additional authorities or resources may be required.

National Defense Strategy

The 2018 NDS moved beyond the "two-war construct" that guided defense strategy, capability development, and investment for the three prior decades, and refocused DOD on "great power competition and conflict" with China and Russia as the primary challenges with which the United States must contend, together with the imperative of deterring and countering rogue regimes like North Korea and Iran. Finally, the framework emphasizes the defeat of terrorist threats to the United States and the consolidation of gains in Iraq and Afghanistan, while moving to a "more resource sustainable" approach to counterterrorism.

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

I believe the NDS accurately assesses the strategic environment and the prioritization of threats based on current geopolitical trends. We are in an era of great power competition; China and Russia continue to be our top strategic competitors and are the most advanced threats in all domains.

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

The DISE provides the intelligence and security support underpinning the NDS lines of efforts of lethality, partnerships, and reform. Reorienting and operationalizing defense intelligence analysis and collection for great power competition; building a modern and resilient intelligence and security infrastructure; modernizing the intelligence workforce; effecting leveraging commercial technologies to maintain a technology advantage, leveraging international partnerships; and operating as a combined enterprise, in my view are the roles and functions that the DISE achieves in implementing the NDS.

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

DISE support is critical to the success of the NDS. I understand that OUSD(I&S) leverages the Combat Support Agency Readiness Review Teams (CSARRT) of the Joint Staff to access enterprise readiness across all mission sets. If confirmed, I will support these efforts and continue OUSD(I&S) efforts and support Departmental efforts to continue to seek ways to increase NDS implementation reforms.

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

I understand that OUSD(I&S) possesses significant expertise for the evaluation of Enterprise readiness. If confirmed, I will review the analytic tools and specific expertise available to OUSD(I&S) to evaluate the readiness of the DISE in order to make an informed assessment.

33. At proposed Fiscal Year (FY) 2021 funding levels, what resource shortfalls are likely to hamper the Defense Intelligence and Security Enterprise's execution of the NDS, in your view?

It is my understanding that the Department has realigned MIP resources to better support the NDS, and the FY 2021 MIP budget request, if supported by Congress, will further the Defense Intelligence and Security Enterprise's execution of 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 OSD(I&S) staff to identify resource shortfalls likely to hamper the DISE's execution of the NDS as they emerge.

34. 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?

It is my understanding that the Department is still making adjustments to its warfighting capabilities to support the NDS. If confirmed, I will work across the Department to ensure any DISE capability gaps and shortfalls are identified and resourced throughout the PPBE process.

35. If confirmed, what changes or adjustments, if any, would you advise the Secretary of Defense and the USD(I&S) to make in the Department's implementation of the 2018 NDS as regards the domains of intelligence and security?

I am supportive of the tremendous efforts the Department has made to date in implementing the NDS. If confirmed, once I am up to speed on efforts to execute the forthcoming Defense Intelligence Strategy, I will assist the USD(I&S) in developing recommendations for the Secretary of Defense. It is critical that all efforts continue to accelerate DISE support to the Department's posture for great power competition.

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

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

The DISE provides direct intelligence and security support to the NDS lines of effort. The DISE assists the Department in gaining and maintaining competitive advantages by prioritizing intelligence support to strategic competition and influence efforts and providing tailored intelligence to DoD research, engineering, and acquisition communities by optimizing intelligence collection and analysis. Additionally, if confirmed, I will work in concert with the broader IC to ensure integration and to leverage collective efforts.

37. What revisions or adjustments would you recommend that the Secretary of Defense make to the 2018 NDS when next he submits to the Congress the assessment required by section 113(g)(1)(F) of title 10, U.S. Code? Please explain your answer.

If confirmed, I will work with the USD(I&S) and his staff to recommend any adjustments, as appropriate, to the 2018 NDS. Since 2018, the NDS has been the guiding document for the Department as it has made tough decisions to focus on great power competition while still ensuring its vital homeland defense mission. The last two years have demonstrated that China and Russia continue their efforts to overturn the rules based international order and the focus of the NDS remains valid. In this light, I will assist the USD(I&S) in making any recommendations to the Secretary of Defense.

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

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

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

Although I do not know the leaders personally, from my time on the National Security Council, I am knowledgeable of our existing intelligence relationships with our Commonwealth Partners (United Kingdom, Australia, Canada, and New Zealand), the North Atlantic Treaty Organization (NATO), and many of the bilateral and multilateral international security partnerships around the globe. These alliances and strategic partnerships are critical to the National Defense Strategy (NDS) and expanding our shared understanding of threats and focus on strengthening our intelligence access and insight into China and Russia.

I am familiar with OUSD(I&S) ongoing efforts to expand intelligence collection sharing on NDS priorities in order to leverage complementary capabilities, economize resources, and improve our mutual understanding of the security environment. In 2019 alone, I understand that OUSD(I&S) has worked to significantly improve defense intelligence partnerships with senior foreign intelligence and counterintelligence leadership in 36 countries through 95 formal key leader engagements. If confirmed, I will support OUSD(I&S) efforts to strengthen these important relationships.

39. 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?

My time in the Army Special Forces taught me the immense value in close partnerships with foreign partners. Strong international relationships and intelligence sharing during my military service resulting in increased mission success and decreased risk to force, while shedding light on the fidelity of strategy, is the foundation for my appreciation of their value at the national level. If confirmed, I will lead the DISE to work closely with international partners to form combined, integrated communities and coalitions that address our most important Defense intelligence and security missions together. I will prioritize mission partnerships where partners enjoy a comparative advantage and there is high potential for return on investment, specifically as they relate to filling intelligence and counterintelligence gaps against China and Russia. I will strive to achieve maximum information sharing, consistent with national policy, with our closest intelligence partners through effective disclosure policies, processes, and enabling informational technologies. Through OUSD(I&S)'s Defense Intelligence Partner Engagement Synchronization Board (DIPE), I will also ensure we synchronize internally on enterprise engagement with foreign partners and that our approach is well-coordinated with consistent messaging.

40. If confirmed, what factors would you consider in rendering decisions on the disclosure and release of military intelligence to foreign governments and international organizations?

Classified military information, including military intelligence, is a national security asset that must be conserved and protected. I would stringently apply the set of criteria required by National Disclosure Policy-1 to synchronize military and national intelligence foreign disclosure policies. NDP-1 criteria includes such factors as consistency with U.S. foreign policy and national security objectives concerning the recipient government or organization; a clearly identifiable advantage or benefit to the U.S. resulting from the disclosure; the ability and willingness of the foreign recipient(s) to protect the intelligence comparable to U.S. safeguards for the classification level of the information; and that the foreign recipient will use the intelligence only for the purpose for which it is being disclosed and not in a way harmful to U.S. interests.

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.

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

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

42. 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? If so, how?

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

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

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

Consideration of both DOD and IC requirements is central to the USD(I&S) role and if confirmed, I will work to maintain open communication throughout this process. OUSD(I&S) facilitates the common gatekeeping function between the Joint Capabilities Integration and Development System and the Intelligence Community Capability Requirements Process. I look forward to working closely with the Joint Staff and JROC during the requirements validation process for NRO capabilities because these systems provide critical intelligence for the warfighter.

The streamlined middle-tier acquisition authorities enacted in Section 804 of the FY 2016 NDAA seek to speed fielding of advanced technologies and systems.

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

I believe that technological discoveries and development are outpacing DoD's ability to modernize and field capability under 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. This authority has provided a pathway for the DISE to develop, test, and field emerging technology to maintain pace with, or counter, adversary capability development.

One of the challenges facing many acquisition programs—ranging from weapons systems to business systems—is unrealistic and infeasible technical requirements.

45. What best practices can the Department employ to generate realistic and technically feasible requirements in the domains of intelligence, counterintelligence, and security?

Collaboration across DoD and the IC is key to developing executable technical requirements for intelligence, counterintelligence, and security. We must ensure intelligence support to acquisition is resourced to deliver technical insights of adversary systems for our weapons development and counterintelligence (CI) /security efforts to protect our critical technologies. Without this support, our new systems may be compromised and unable to compete against our adversary's systems, and finite resources misallocated. If confirmed, I will work to ensure we provide the required intelligence and security resources that is feasible to support modernization of new weapon systems and protection of our critical technologies. I also believe the Department can continue to benefit from a close relationship with industry. By working together throughout the entire process, requirements can be shaped based on shared information and innovative commercial solutions as well as the underlying intelligence.

Intelligence Support to the Warfighter

46. If confirmed, how would you balance the need to provide intelligence support to the warfighter with the need to provide intelligence support to policy makers?

My understanding and belief is that balancing these needs is one of the OUSD(I&S)'s primary responsibilities. In today's environment of global and regional threats, most issues are relevant to both warfighting commands and policy makers. Where there remains tactical and operational differences, if confirmed, I would work to ensure the DISE continues to satisfy requirements for operationally–relevant intelligence that directly enable warfighter success, and I would work collaboratively across DoD and with interagency partners to inform policy and military decision-making by our national leaders.

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

My experience both in uniform and serving on the National Security Council staff underpins my belief in the importance of and the continued opportunity to improve collaboration across the intelligence community to better support the warfighter. If confirmed, I would engage early and often with the combatant commanders to improve my understanding of their needs, and I would frequently engage leaders within the national intelligence community to obtain support to meet those warfighter needs. I am particularly interested in applying greater attention to faster, more agile and adaptive processing, exploitation, and dissemination of intelligence data to better support the warfighter and others that engage our adversaries at the tactical edge. A few specific opportunities to improve and leverage intelligence support to warfighters include

integrating Artificial Intelligence and Machine Learning, developing resilient architectures, and robust interoperable coalition networks.

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

I understand that in conducting policy oversight, OUSD(I&S), working in coordination with the Joint Staff to conduct annual reviews and assessments of intelligence assets and resources at the Combatant Commands and the Combat Support Agencies. This ensures the DISE is assessing and prioritizing intelligence needs, and is responsive to the requirements of the operating forces. If confirmed, I will support this proven process, while also seeking out new ways to ensure the Commands prioritize and receive the intelligence support they require.

49. In your view, are the Joint Intelligence Operations Centers and Service Intelligence Centers organized and resourced to most effectively support warfighter requirements under the NDS, to include support to joint targeting for the combatant commands? What changes, if any, would you recommend?

Given the available resources, I believe that the Joint Intelligence Operations Centers (JIOCs) and Service Intelligence Centers (SICs) are appropriately resourced. JIOCs and SICs do a variety of missions, task, activities, and functions. I understand that recent USEUCOM and USINDOPACOM resource increases were important steps to support the targeting capabilities of the combatant commands. If confirmed, I will support periodic review and alignment efforts as it is an important effort to ensure effective use of resources in support of the warfighter.

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

From my time in the Special Operations community, I appreciate the key differences between tactical, defense, and national intelligence missions. Timely and accurate information/intelligence is critical for Special Operations Forces conducting tactical operations. 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.

Defense and national intelligence serves a more strategic role—they support departmental and national objectives, and are integrated with all instruments of national power. Intelligence agencies from national level also develop and maintain intelligence databases that are also used by SOF intelligence personnel to provide an initial intelligence estimate.

Special Operations Forces missions require accurate, detailed, and timely intelligence that only integrated, multi-disciplined collection and analysis can provide.

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 Nation.

51. If confirmed, how would you ensure that intelligence activities carried out by special operations forces are properly coordinated with activities carried out by the Intelligence Community?

I recognize the importance of fully coordinating special operations forces' intelligence activities with those of the intelligence community. I would, if confirmed, work closely with the ASD SO/LIC and the DoD Senior Intelligence Official to ensure SOF intelligence activities comply with law and policies, and coordinate to deconflict and leverage each other's activities to meet intelligence needs from the tactical to the strategic levels.

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.

52. What is your understanding of efforts by the OUSD(I&S) to leverage information technology and innovative concepts to develop an interoperable, joint command, control, communications, computer intelligence, surveillance, and reconnaissance architecture and capability to support the warfare of the future?

It is my understanding that the USD(I&S) is developing a Defense Intelligence Strategy (DIS) that leverages the published data strategies of the IC and the DoD to optimize the use of information technology and emerging innovative concepts to modernize and transform the entire DISE. It is also my understanding that the USD(I&S) is a full participant in the Department's Joint All Domain Command and Control (JADC2) initiative intended to connect distributed sensors, shooters, and data from and in all domains to all forces.

If confirmed, I will continue to work closely with the DNI and across the Department to ensure that all defense intelligence capabilities achieve architectural superiority, as envisioned in the NDS, and remain in lockstep with the emerging C4ISR architecture.

53. 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 that Project Maven aims to enhance human capability through human-machine teaming through the Maven Smart System, which fuses operational and intelligence on an interface thereby significantly reducing time needed to process and exploit data. Maven brings a step change in performance of the human- machine team reducing decision making cycles to a fraction of the time required without AI assistance. Reduced cycle times increase the speed of combat and allow warfighters to engage more targets more accurately and with greater efficiency.

On April 26, 2017, the Deputy Secretary of Defense established an Algorithmic Warfare Cross-Functional Team under the oversight of the USD(I&S). The Deputy further directed the USD(I&S) to consolidate all intelligence initiatives to develop or field Artificial Intelligence, automation, machine learning, deep learning, and computer vision algorithms.

54. What is your understanding of the progress the OUSD(I&S) is making in consolidating these initiatives across the Department? Has consolidation yielded any benefits, in your view? Has consolidation resulted in any unanticipated disadvantages? What more remains to be done? Please explain your answer.

I understand that the USD(I&S) has made significant progress in highlighting the need for AI integration across the Department. Project Maven has been a key pathfinder for the Department, heavily shaping intelligence and AI efforts for the DISE. The immediate benefit is energizing the DISE and other DoD organization to recognize the need for immediate AI integration and the need for the Department to embrace the transition to machine-enabled systems. The Joint AI Center (JAIC) is an important step in the right direction; however, the key work that remains for the Department is to embrace a "culture change" in integrating AI into all aspects of how we fight, how we conduct intelligence exploitation, and how we do business. Integrating AI into our current workflows will spawn efficiency, speed, and cost savings.

55. What is the relationship between the Algorithmic Warfare Cross-Functional Team and the Joint Artificial Intelligence Center that reports to the DOD Chief Information Officer?

The Algorithmic Cross Functional Team ((AWCFT), which is also known as Project Maven, and the Joint Artificial Intelligence Center (JAIC) share a close relationship. While the AWCFT is focused on AI in the DISE and intelligence-related functions, the JAIC is charged with accelerating the delivery of AI-enabled capabilities to the DoD, scaling the Department-wide impact of AI, and synchronizing DoD AI activities to expand Joint Force advantages. I understand that the activities of the two organizations are linked as the AWCFT is conducting test and fielding operations for integrating AI-enabled algorithms into our workflows, and the JAIC is creating the environment for the Department to be ready to accept the full integration of AI at scale across all Department functions, primarily for non-intelligence functions and missions.

In a February 27, 2020, *New York Times* Op-ed, Eric Schmidt, the chairman of the National Security Commission on Artificial Intelligence and the Defense Innovation Board, 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."

56. How should the OUSD(I&S) resolve private sector concerns about how—if at all—the technology community should go about participating in the innovation and development of innovative capabilities to be used by the United States in warfare and/or in non-kinetic conflict?

The integration of technology and innovative capabilities aims to only make human decision making better, with less error, more certainty, and less collateral damage. I do not believe we are at the point where machines can or should make decisions without a human in the loop; instead, technology will provide the human decision maker with the best information available to decrease the time required to make decisions with greater accuracy and precision. AI-enabled technologies will provide our decisions makers with the surest information and best accuracy that we have ever experienced in the history of warfare.

Demand for intelligence, surveillance, and reconnaissance (ISR) capabilities of every kind has grown exponentially in recent years largely due to the enhanced situational awareness and targeting capabilities ISR brings to our commanders. Almost all of the geographic combatant commands have validated ISR requirements that are not being met. Since 9/11, U.S. Central Command (CENTCOM) has received the overwhelming share of ISR assets, yet a process that consistently ranks even the lowest priorities of one combatant command higher than the highest priorities of most others inevitably invites skepticism.

57. What is your assessment of the adequacy of the Global Force Management Process (GFMAP) as DOD's means of allocating ISR assets to the combatant commands?

I understand that the Global Force Management Process (GFMAP) was designed to allocate forces and capabilities across the Combatant Commands to best meet their prioritized requirements, including allocation of ISR assets. I understand that one major challenge in this process has been how to best prioritize the allocation of ISR assets against competing Combatant Commanders requirements which far exceed the Department's available ISR resources. Based on my own experience in combat, I understand the rightful insatiable demand for ISR due to its ability to significantly improve mission success and reduce risk to force. I believe that close coordination with the Chairman of the Joint Chiefs of Staff is imperative to support a process that balances ISR allocation prioritizing great power competition in support of the NDS along with

those Commands in active combat zones and force protection requirements. If confirmed, I will work to help optimize this trade space.

58. In your view, should the GFMAP process for allocating ISR assets be modified in any way? Please explain your answer.

If confirmed, one of my first duties will be to study how the GFMAP process is occurring, with the goal of understanding how the allocation of ISR assets aligns with Department priorities as outlined in the NDS. I will work closely with the Secretary of Defense and the Chairman of Joint Chiefs of Staff to ensure ISR allocations reflect current NDS prioritization through the GFMAP process.

59. What arguments would you use to advocate for additional ISR and like enabling assets, if confirmed?

Requirements for DoD have shifted with the NDS to focus on great power competition and the ability to operate in denied environments. As such, DoD continually seeks the best ISR and enabling assets to meet those needs. If confirmed, I will work with our Combatant Commanders and the Services to determine how defense intelligence can best support warfighter requirements for additional ISR assets and capabilities to address these concerns.

Counterintelligence, Law Enforcement, and Security

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

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

61. 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?

The USD(I&S) has broad responsibility for oversight of DoD counterintelligence (CI). This includes development and oversight of Department CI policy, programs, guidance, and training of CI personnel. OUSD(I&S) works closely with the Defense

Intelligence Agency for development of CI strategies and supporting campaigns to ensure alignment with national level priorities. The USD(I&S) is a standing member of the National CI and Security Center's CI EXCOM, and through this organization, coordinates and collaborates within the U.S. Government. If confirmed, I will play an active role with my government counterparts to work to ensure the right balance of CI roles and responsibilities exists across the federal government.

62. What is your understanding of progress that has been made in transitioning DOD's law enforcement policy function from the OUSD(P&R) to the OUSD(I&S)?

To the best of my knowledge the transfer of responsibility is complete. The transition included the USD(I&S)'s responsibility to carry out the Secretary of Defense's responsibilities for the protection of DoD buildings, grounds, property, and persons under 10 U.SC. § 2672.

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

I understand the integration of the security professionals and practices of intelligence, counterintelligence, and law enforcement components has strengthened the Department's security posture. Working side by side with security professionals allows law enforcement professionals to develop effective policies, standards, and repeatable procedures, and sufficient controls to deter and deny our strategic competitors malign actions. As these communities continue to work together more effectively, our information and technologies will be better protected.

64. 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?

U.S. law and policy provides guidance on limits for DoD intelligence activities pertaining to U.S. persons and the protection of the Constitutional rights of all Americans. It is my observation that the USD(I&S) has effectively organized the DISE to ensure appropriate separation between intelligence and security functions. If confirmed, I will ensure that all intelligence and security activities are conducted in a manner that respects civil liberties and protects the rights of Americans enshrined in the Constitution, which I have many times taken an oath to defend.

65. 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?

Although I am not intimately familiar with all of the authorities necessary to execute the law enforcement policy function at this time, I understand that the Department has the necessary authority under 10 U.S.C. § 2672, and that upon Attorney General approval,

law enforcement guidelines will be issued for further implementation of the statute. If confirmed, I will work to ensure the DoD law enforcement community receives what it needs from OUSD(I&S) to effectively exercise any authorities which have been delegated.

In his role as 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.

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

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

<u>Security Clearance, Suitability, and Credentialing Reform</u>

On September 29, 2019, the National Background Investigation Bureau (NBIB) was realigned from the Office of Personnel Management (OPM) to the Defense Counterintelligence and Security Agency (DCSA).

67. What is your understanding of progress the OUSD(I&S) made in implementing the Trusted Workforce 2.0 initiative?

I understand that OUSD(I&S) continues to work closely with the Security Executive Agent (SecEA), Suitability Executive Agent (SuitEA), and the Performance Accountability Council (PAC) Performance Management Office (PMO) to fully define Trusted Workforce 2.0 and to make incremental changes in advance of full implementation. These efforts have resulted in the enrollment of more than half of the DoD cleared workforce in Continuous Evaluation (CE), which will enable the discontinuation of traditional and costly periodic reinvestigation practices.

68. How many DOD personnel are presently enrolled in continuous vetting? How has the OUSD(I&S) validated the accuracy and reliability of its continuous vetting programs and processes as compared to the outcomes of standard "in person" periodic background investigations?

I have been told that, as of July 20, 2020, the DoD population enrolled in its Continuous Evaluation program is approximately 2.3 million, and the population enrolled in its Continuous Vetting program is approximately 141,500. I understand that shifting away from costly and time consuming periodic reinvestigations is enabling the Department to identify concerns earlier than would be found by using the traditional five year periodic reinvestigation without any degradation in investigative findings. Moving to a continuous vetting environment and using innovation to automate many of these processes should allow the Department to more effectively and efficiently identify and mitigate alerts far sooner in the process. If confirmed, I will work with the OUSD(I&S) staff to ensure process implementation is informed by sufficient accuracy and reliability validation.

69. What is the current number of backlogged background investigations for Secret and Top Secret Security clearances?

I have been told that the current background investigations inventory is approximately 202,300 which is a combination of the traditional "Tiered" investigations and other checks requested by Federal agencies. The total T3 (Secret) inventory is currently approximately 60,500 and T5 (Top Secret) is approximately 25,300. The background investigations inventory has improved by 53% since 2019 and the DoD CAF has improved its adjudication inventory by 52% since its high in 2019.

I believe that although the Department has made great progress in reducing the inventory, more work must be done to ensure background investigations are completed in a timely fashion. I understand this is a high priority for the Secretary and Deputy Secretary, and if confirmed, I will ensure the Defense Counterintelligence and Security Agency continues its progress towards the timeliness requirements set forth by OMB and Congress.

70. At present, how long is the background investigation and adjudication process for each such level of clearance?

I understand that the target goal for an initial T5 (Top Secret) is 80 days, and the target goal for an initial T3 (Secret) clearance is 40 days. I understand that currently the initial T5 process averages 91 days, an improvement of 59% since First Quarter of FY20, and the initial T3 process averages 52 days, an improvement of 65% since First Quarter of FY20. The DoD Central Adjudication Facility adjudication process has improved by 70% since the beginning of First Quarter FY20, achieving a current adjudication inventory of approximately 74,800.

71. In your view, what should be the "appropriate" goal for the number of active background investigations ongoing at any given time, and how long do you project it will take to achieve that goal?

As the Department and the government continue to define and move toward full implementation of TW 2.0, I believe it is reasonable to define new timeliness goals

appropriate for the new processes supporting initial background investigations. If confirmed, I will engage with the SuitEA and the SecEA on the question of appropriate timeliness goals for initial clearances; weighing process optimization, required resources, and department impact.

72. What new standards will be used to investigate and adjudicate derogatory information about clearance holders in DOD?

Although I am not intimately familiar with all of the details of TW 2.0, I understand that it will include new investigation and adjudication policy. If confirmed, I will ensure that OUSD(I&S) continues to work closely with the policy makers at SecEA and SuiteEA to frame the national policy and implement those new standards once authorized.

73. How will DOD rationalize its new approach to security, suitability and credentialing background investigations and adjudication with processes employed by the Intelligence Community?

As I understand it, all Federal agencies use a common set of investigative and adjudicative standards, therefore DoD is aligned with the processes employed by the Intelligence Community. DoD continues to partner with members of the Intelligence Community to maximize the exchange of personnel security information and thereby minimize any duplication of investigative or adjudicative effort.

74. How will suitability-related information pertaining to a candidate for employment with DOD be transmitted to human resources personnel and hiring officials, and what training will be provided to such personnel in how to apply the information they receive?

I believe the DoD suitability program falls under the authority of the Under Secretary for Personnel and Readiness. However, as DoD transitions to a continuous vetting environment, partnerships among the officials responsible for security, suitability and credentialing will be essential.

75. If confirmed, how would you use the Defense Personnel and Security Research Center (PERSEREC) to improve personnel suitability, security, and reliability policies and practices?

I understand that PERSEREC is a valued partner to USD(I&S) and is respected and utilized at the Federal level in framing the TW 2.0 activities. Research conducted at PERSEREC has been and will continue to be used by policy makers as they modernize the vetting enterprise.

76. If confirmed, how would you ensure that DCSA is highly responsive to the needs of the USD(A&S) for vetting DOD contractors in responsibility determination?

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

Insider Threat

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

77. 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 nor have access to these systems, I believe it is imperative that DITMAC and the DoD Insider Threat Enterprise have access to data from across these various relevant pillars to identify and mitigate potential threats from insiders. If confirmed, I will lead a continuous effort to eliminate stove-piping and remove barriers to data sharing, as allowed by law.

78. How should insider threat architecture and activities overseen by USD(I&S) be integrated and coordinated with the Department's cybersecurity architecture and activities, in your view?

OUSD(I&S) maintains a close relationship with the office of the DoD CIO, which fosters integration and collaboration relevant to insider threat and cybersecurity. If confirmed, I will work to ensure this relationship continues and seek ways to enhance our efforts to find areas of common interest, force multiplication, and efficiencies.

79. 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?

I have not been made aware of any authorities that USD(I&S) lacks with regard to technological advances in integrating information regarding insider threats. I believe OUSD(I&S) staff are well-situated to provide policy, oversight, and guidance for the spectrum of Counter Insider Threat efforts, including the development of technological solutions. If confirmed, I will ensure OUSD(I&S) continues to establish guidance to the enterprise to continue innovating to ensure the most effective approaches to information integration are being utilized to identify insider threats.

80. 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? Does the USD(I&S) require any additional authorities or resources to resolve these challenges effectively and expeditiously?

I believe that DoD experiences the same challenges faced by many organizations both private and public when developing large scale information technology systems responsible for the ingest, dissemination, and retention of large volumes of data with interfaces across numerous platforms. At this time, I do not believe that the Department requires additional authorities to design, develop, and implement information technology systems for personnel security or Insider Threat. However, if confirmed, I will assess whether additional authorities or other resources are needed for USD(I&S) to optimally address these threats.

81. What is your understanding of the cultural and organizational resistance to improvements in the personnel security processes and insider threat detection and prevention in DOD? Does the USD(I&S) require any additional authorities or resources to address these challenges effectively and expeditiously?

It is my experience that there's always resistance to change in any organization. I believe, however, that there is wide acceptance across the Department that we need to modernize personnel security and implement insider threat policy to more effectively safeguard personnel, information, and facilities. I am not aware of any identified gaps in authorities and resources, but if confirmed I will assess whether additional authorities or other resources are needed for USD(I&S).

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

Given my industry experience, I understand the security perspective of DoD contractors, and believe I will be able to serve as a critical liaison to industry from the Department on the full scope of insider threat issues. While I am not currently serving in a government position, I understand that at this time, given the thousands of DoD contractors and their associated data systems, the ability to integrate DITMAC into their systems is not

feasible. However, an immediate alternative may be to develop and sustain a strong, consistent flow of information sharing between cleared industry and DITMAC through existing DCSA industrial security and vetting mechanisms. Ultimately, both the U.S. Government and industry share mutual goals of improved information sharing and ensuring trusted workers and architectures, programs, and policies should continue to align incentives. If confirmed I will look forward to tackling this issue, which I recognize is of great priority to the Congress.

83. In your view, how will DOD's newly-designated Defense Counterintelligence and Security Agency (DCSA), better posture the Department to deter, detect, and mitigate insider threats before they harm national security?

The designation and continuing transformation of DCSA brings together two national security missions instrumental to deterring, detecting, and mitigating threats to the Department. This enables these separate but complementary missions to more easily share data, coordinate necessary actions, and streamline processes and capabilities to deter, detect, and mitigate insider threats. If confirmed, I look forward to working with DCSA to ensure this new organization reaches its full potential.

84. What progress has DOD made in identifying career paths and training programs for the development of insider threat expertise and the advancement of insider threat prevention personnel?

DoD senior leadership is committed to continually expanding the growth in expertise for practitioners who directly execute counter insider threat functions across our enterprise. It is my understanding DoD has established and continues to offer training, education, and awareness courseware through organizations such as DCSA's Center of Development for Security Excellence and others. In addition, efforts continue in the development of specialized educational curriculum and tradecraft, and the establishment of nationally accredited certification programs. If confirmed, I will continue to support and expand these efforts.

85. 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?

OUSD(I&S) has engaged all of DoD about the importance of this issue, and is the key sponsor for National Insider Threat Awareness Month each September. If confirmed, I would continually engage Department-wide to ensure that their insider threat programs are in compliance with policies, procedures, training, and reporting requirements. Furthermore, if confirmed, I will advocate to secure funding and manpower resources on behalf of DoD to support this critical mission.

86. Has the Defense Biometrics Identification System (DBIDS) been implemented at all installation gates and access control points—DOD-wide—to ensure that personnel

and visitors are properly vetted prior to entering a military installation? If not, what is the cause of delay?

The DBIDS is one of several electronic physical access control systems in use at DoD to ensure that only authorized, properly-vetted personnel and visitors are granted access to DoD installations. I understand that USD(I&S) has established baseline requirements for ePACS, but has not directed the use of any particular system to allow the DoD Components to employ the system that best meets their needs and to allow industry to offer innovative new solutions. I understand the DBIDS solution has been implemented at all regularly-used installation gates and access control points for Air Force, Navy, Marine Corps, and Defense Logistics Agency installations. The Pentagon Force Protection Agency has implemented a commercial ePACS at the Pentagon Reservation and associated facilities. The Army has implemented DBIDS at approximately 5 installations and another solution, known as Automated Installation Entry (AIE), at approximately 35 installations. I believe the Army has approximately 70 installations that do not yet have an ePACS. I am told that OUSD(I&S) is working closely with the Army to understand the reasons for the delay in implementing an ePACS, whether DBIDS or AIE, at the remaining installations and to accelerate the timeline for doing so.

87. How will the new vetting policies and processes applicable to foreign military students enrolled in DOD training and educational programs mitigate risk to U.S. personnel, facilities, and equipment?

Following the terrorist attack at Naval Air Station Pensacola in December 2019, DoD recognized it needed to improve vetting for International Military Students. Consequently, the Secretary of Defense directed a Security and Vetting Review to look at the full range of procedures from initial application, to arrival in the United States, and daily access to DoD training facilities. This review resulted in significant changes to ensure that an appropriate background check is conducted as a condition of gaining access to DoD facilities. This is complementary to, but separate and distinct from, the State Department visa process. If confirmed, I will work to ensure that this process, plus a suite of new procedures at the installation level, aligns IMS screening and vetting more closely with that which DoD applies to U.S. personnel accessing DoD facilities and will strengthen DoD's overall security posture.

The National Security Innovation Base

The Department of Defense is pursuing a wide-ranging strategy to engage with commercial entities engaged in cutting-edge research and development. The Department recognizes that it needs new acquisition policies and practices to enable the Department to engage the private sector with the necessary speed, agility and flexibility. Two related obstacles are the time and difficulty involved in the security clearance process and the hurdles that non-traditional contractors face in getting access to data to test and demonstrate new information technology and software. The National Geospatial-Intelligence Agency (NGA), for example, concluded that it lacked the authority to share

even its unclassified imagery data with companies and universities it hoped could develop dramatically improved exploitation capabilities through machine learning-based artificial intelligence algorithms.

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

In order to support the innovation activities critical to the Department, there must be concerted effort supporting both the 'promote' and 'protect' pillars of our National Security Innovation Base. The Department relies on U.S. academia and innovation centers throughout the country to invest in science and technology that will maintain the lethality of our joint forces and enable our allies to defend their own national security. If confirmed, I will collaborate with the private sector, academia, and other government organizations to identify new ways of unlocking our innovation advantage while ensuring we also protect it. Protecting our innovation at every level of the development chain is critical to maintaining our technology advantage. Identifying security measures that support the very innovation that is necessary to protect is critically important. Properly considered, properly applied, and continuously managed security practices themselves are a critical, enabling element in research and innovation to encourage lawful competition and to protect U.S. interests. If confirmed, I will continue efforts across the Defense Security Enterprise that balance evidence-based innovation with both time-tested, "traditional" and innovative approaches to security. If confirmed, I will support efforts that enable the Defense Intelligence and Security Enterprise to continue to evolve, innovate, and tailor practices to ensure innovation can flourish in an era of enduring strategic competition from U.S. adversaries.

By memorandum of October 24, 2018, then-Secretary of Defense Mattis established the Protecting Critical Technology Task Force, 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.

89. Does the OUSD(I&S) participate in the Task Force, and if so, what functional expertise does the OUSD(I&S) bring to the table?

I am told that OUSD(I&S) provides two full-time detailees to the Protecting Critical Technology Task Force. These representatives embody the expertise inherent in OUSD(I&S) with over 50 years of combined experience in the Intelligence Community, counterintelligence expertise, and security enterprise involvement. If confirmed, I will ensure OUSD(I&S) continues to support all of the Department's efforts to protect our technology and innovation advantage; to include disrupting strategic competitor access to advance Defense technology.

90. What were the outcomes of the Task Force's 30- and 90-day sprints?

I understand that OUSD(I&S) completed or adapted the tasks assigned in the Task Force's 30- and 90-day sprints. One of the key successes was the publication of DoD Instruction 5200.48, *Controlled Unclassified Information*, that established the roles and responsibilities for the Defense Components' storing, handling, marking, and dissemination of Controlled Unclassified Information (CUI). Institutionalizing these procedures will ensure CUI for critical programs and technology are better protected from our strategic adversaries. In addition, I understand OUSD(I&S) is developing policy to elevate the protection of critical programs and technology using counterintelligence, intelligence, and security authorities. If confirmed, I will ensure that OUSD(I&S) continues to accelerate and institutionalize critical technology protection for the Department.

91. How does the OUSD(I&S) verify contractor compliance with OPSEC requirements incorporated in classified contracts?

OPSEC is a critical "General Countermeasure" factor in program protection planning, with requirements and specific countermeasures and protection capabilities coming together as programs mature toward milestone decisions. I understand that OUSD(I&S) sets overall DoD-level OPSEC policy and the DoD Component OPSEC program managers work closely with their respective contracting offices to ensure compliance. Component-level OPSEC program managers are best suited to conduct verification, supported by OUSD(I&S) oversight and coordination, due to their visibility into program protection requirements and mission needs.

92. 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?

A major feature of this era of great power competition is the threat posed by adversary theft of critical technologies and innovative advancements often through the compromise of classified information. China especially demonstrates the will and capacity to obtain— either legally or illegally— or otherwise compromise U.S. and allied technologies to further their own strategic objectives. In order for the United States to both continue to be the world's innovative leader and to retain the advantage it provides, I believe that is essential for our intelligence, counterintelligence, and security enterprises to maintain a heightened diligence in identifying and responding to adversary threats to the National Security Innovation Base.

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

The National Security Innovation Base (NSIB), outlined in the White House issued National Security Strategy (2017), includes academia, national laboratories, and private sector companies that contribute to U.S. innovation and national defense. The Defense Industrial Base (DIB) only represents a portion of the entities critical for the innovation required for sustaining a defense technology advantage. Essential elements that do not traditionally do business or have direct contact with the Department of Defense (DoD) lack access to key security benefits, awareness and training, and intelligence and information sharing that comes with directly participating in DoD's supply chain. In areas identified critical for defense technology priorities, defense activity should be aligned to the entire technology ecosystem; ranging from startups, universities, to large defense contractors. As activity expands past traditional DIB entities, close coordination with interagency partners will become increasingly important. If confirmed, I will support DISE efforts to align DoD efforts to best promote and protect the NSIB and pursue additional resources if critical shortfalls are identified.

94. How would you propose to improve the support provided by the DCSA, the DOD counterintelligence organizations, and the national Intelligence Community better to 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?

I believe that DoD's partnership with the National Security Innovation Base can be strengthened through information sharing and programs and policies which align incentives for NSIB entities to enhance our combined visibility and understanding of potential threats deeper into supply chains. A National Security Innovation Base that is better informed of the activities that comprise the threats we face is better postured and willing to implement necessary security practices. If confirmed, I will continue to explore ways DCSA and other DoD counterintelligence organizations can more timely and effectively share information with the National Security Innovation Base and align incentives with non-traditional NSIB entities.

Collection & Special Programs

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

It is clear the technology environment today has created pressing challenges to conduct some traditional collection activities. The volume of commercially available data on individuals and their activity and the proliferation of both networked, correlated, and automated systems as well as algorithms that can exploit the information pose a risk to our human intelligence collection activities.

If confirmed, I would work to ensure that sufficient focus and resources are devoted to Defense Intelligence and Security Enterprise efforts to address these ubiquitous realities and pursue additional resources if there are critical technical and human intelligence collection shortfalls. These challenges are not unique to the Department and, if confirmed, I would work with our IC partners to integrate and synchronize DoD and IC efforts and resources for addressing these threats.

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

I believe the major challenges confronting the Department include adapting to and providing timely awareness and insights into a diverse, complex and ever-changing array of security challenges. If confirmed, I will support OUSD(I&S) continued review of processes and policies to support the changing environment. This may require changes in how DoD personnel train and use tradecraft, technologies, methodologies, and processes to collect intelligence. Aggressive efforts to ensure DoD is leveraging the best commercial technologies will remain essential. Focus should remain on our ability to rapidly field technologies where required. If confirmed, I will work to ensure that OUSD(I&S) addresses these evolving challenges in a manner which continues to protect our intelligence sources and methods.

Intelligence Oversight

97. 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 OUSD(I&S) is the Principal Staff Assistant and advisor to the Secretary of Defense regarding intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters. This includes exercising authority, direction, and control on behalf of the Secretary of Defense over certain defense intelligence components of the Department of Defense and working closely with the Joint Staff, Combatant Commands, Service components and the ODNI to develop effective policy, plans, programs, and priorities. In direct coordination with the DoD Senior Intelligence Oversight Official and Office of General Counsel, OUSD(I&S) needs to ensure that defense intelligence sensitive activities across the Department are conducted consistent with law and DoD policy.

98. How does the OUSD(I&S) engage with the President's Intelligence Oversight Board and on what matters?

My understanding is the DoD Senior Intelligence Oversight Official's (SIOO) has primary responsibility for engaging with the President's Intelligence Oversight Board (PIOB). OUSD(I&S) supports SIOO engagements with the PIOB by reviewing

notifications and reports, and at times assists in briefings. If confirmed, I will continue to foster a collaborative relationship with the SIOO.

Information Operations

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

99. 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 DISE must improve its ability to compete in the information environment and to inform and shape the perceptions of specific audiences in order to gain or maintain a competitive advantage. My view is that the Department should employ defensive activities concurrently with offensive information operations across multiple domains to capture data, process intelligence, and conduct operations that both counter malign actors and advance American advantage. Prioritization of our efforts to deter and defend against strategic information operations should be documented and resources should be focused accordingly.

To maintain preparedness against strategic information operations, I understand the Secretary recently directed the establishment of an effort that will integrate, coordinate, and increase the speed and agility of a broad scope of operational capabilities to address the current strategic environment of great power competition, as outlined in the National Defense Strategy. Efforts to defend against strategic information operations must be a whole of government effort and if confirmed I will work to ensure the DISE effectively integrates Department efforts with our interagency partners.

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

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

I agree and understand that the Department is developing a whole-of-department framework to counter malign influence operations and that this approach has been socialized with the interagency. If confirmed, I will work to support the Department's efforts and continue to work with our interagency partners.

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

My understanding is the DISE is focused on shifting its collection and other activities against both China and Russia. This includes the DISE contributing to efforts that counter Russian influence operations. Developing frameworks that can be rapidly operationalized against key target audiences is one approach that drives collection focus and prioritization. If confirmed, I will continue the USD(I&S)'s emphasis on strategic competition with Russia and China and work to ensure efforts are integrated with the interagency.

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.

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

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

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

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

If confirmed, I will work with Department stakeholders, the DISE, and IC to enable the implementation of the USD(I&S) Defense Intelligence Strategy for Cyberspace

Operations. This strategy provides overarching direction to the DISE in closing gaps with the Cyber Strategy as identified in the 2018 Cyber Posture Review.

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

104. Is it feasible, in your view, for DOD to operate in cyberspace below the level of armed conflict?

Yes, it is both feasible and necessary. Today, the United States' strategic competitors are conducting cyber-enabled campaigns to erode U.S. military advantages, threaten our infrastructure, and reduce our economic prosperity. In particular, strategic competitors China and Russia have expanded competition to include persistent campaigns in and through cyberspace with activities that individually fall below the threshold of armed conflict but collectively pose a long-term strategic risk to the nation, as well as to our allies and partners. As Russian and China implement strategies to achieve their objectives short of armed conflict, it is imperative the United States is able to detect, disrupt, and deter efforts in cyberspace. DoD is an important element of an effective whole of government strategy.

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

I expect that foreign states will continue to use malign influence measures in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic process. As part of a whole-of-government effort, using all elements of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation, DoD and the DISE should be postured to support with forward defense activities. This forward defense should include working with foreign partners, as well as the private sector, academia, and civil society to identify, counter, and prevent the use of social media platforms for malign influence operations, while also respecting civil rights and liberties.

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

Anticipating or responding to cyber attacks on commercial entities is the mission of the Department of Homeland Security (DHS), and I understand that the role that DoD plays in that mission is very clearly defined. DoD is responsible for threat response to DoD cyber incidents affecting DoD assets and the DoD Information Network (DoDIN). DoD can also support civil authorities for cyber incidents outside the DoDIN when requested by DHS when such support is approved by the appropriate DoD official, or directed by the President. Such support would be provided based upon the needs of the incident, the capabilities required, and the readiness of available forces. DoD, thru the DISE, actively characterizes and assesses foreign cybersecurity threats and informs the relevant Interagency partners of current and potential malicious cyber activity. Upon request, the DISE components may provide technical assistance to other Federal Departments and Agencies; other DoD elements may provide support to civil authorities in accordance with applicable law and policy.

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

I understand that the Department has been studying this question closely to ensure that any decision concerning the dual-hat leadership arrangement is fully informed and mitigates potential risks to national security and to the effectiveness of U.S. Cyber Command and the National Security Agency. If confirmed, I will participate in this review, as appropriate, to understand any effects on national security or the operational effectiveness of DoD's capabilities.

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

I believe that a close and continuing partnership between the DoD CIO, the Under Secretary of Defense for Policy, PCA, and the USD(I&S) is essential to best align intelligence policies and capabilities with Policy objectives outlined in the DoD Cyber Strategy implementation plan. I do not currently have sufficient information to have a perspective about the adequacy of the support at this time, however if confirmed, I will ensure OUSD(I&S) remains a valuable partner in the DoD Cybersecurity mission.

Torture and Enhanced Interrogation Techniques

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

Yes, and I believe it represents the values and behavior expected of the U.S. military.

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

My understanding is the Secretary of Defense directed the Under Secretary of Defense for Intelligence & Security (USD(I&S)) to lead a DoD review of the U.S. Army Field Manual 2-22.3 (FM), as required by section 1045 of the National Defense Authorization Act for Fiscal Year 2016. If confirmed, I would assist the USD(I&S) in reviewing the FM help the USD(I&S) formulate recommendations made to the Secretary of Defense based on that review.

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

I am not aware of any provisions in the FM that may need to be revised; that is what the ongoing review will determine. If confirmed, I will work with the USD(I&S) and the OUSD(I&S) staff to ensure that review is thorough. My understanding is that the review is thoroughly examining the intelligence interrogation approaches and techniques in the FM based on lessons learned over the past several years.

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

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

Yes. Section 2441 applies to war crimes, including grave breaches of common Article 3 of the Geneva Conventions, committed by or against a member of the U.S. Armed Forces or a U.S. national. I believe that it is very important to continue to hold ourselves to the highest standards for the humane treatment of detainees, and that we must make clear to our foreign partners that we also expect them to hold themselves to the same standards. It is my understanding that DoD is committed to ensuring the humane treatment of all detainees. DoD Directive 2311.01, "DoD Law of War Program," requires all military and U.S. civilian employees, contractor personnel, and subcontractors assigned to or accompanying a DoD Component to report through their chain of command, or through other channels, such as the military police, a judge advocate, or an inspector general, all reportable incidents, including those involving allegations that non-DoD personnel, including foreign partners, may have violated the law of war. A reportable incident is an incident that a unit commander or other responsible official determines, based on credible information, potentially involves a war crime. The unit commander or responsible official need not determine that a potential violation occurred, only that credible information merits further review of the incident.

Military Accessions Vital to the National Interest (MAVNI) Program and Lawful Permanent Residents (LPR)

113. In your view, do the benefits of the MAVNI and LPR accessions programs outweigh both the potential security risks associated with accessing such applicants into the military and the costs to the Department associated with conducting security, suitability, and reliability screenings of non-citizen applicants? Please explain your answer.

I am aware of the counterintelligence concerns associated with the MAVNI program which led to its discontinuation in 2016. At this time, I do not have sufficient information at this time to assess the value of the MAVNI program relative to the risks it may have posed to national security.

Regarding the LPR program, if confirmed, I will review this program, as appropriate, to ensure that the benefits outweigh the costs of background investigations and any associated risk. Also, I understand the Department is using a new capability for accessions to identify potential foreign influence and foreign preference concerns more effectively.

114. If confirmed, would you recommend reactivation of the MAVNI program and the acceptance of new applicants? What changes—if any—would you recommend to strengthen security, suitability, and reliability-related policies governing a "reactivated" MAVNI program?

If confirmed, I would have to review the relevant classified information related to the MAVNI program to develop an informed view regarding any recommendation for reactivation.

115. In your view, should LPR applicants be subject to the same security, suitability, and reliability screenings as applicants under MAVNI? Please explain your answer.

I believe that all persons entering a national security position should receive the same base-line vetting, as required by national level policy, including LPRs and MAVNIs. Further, I believe that additional vetting criteria should be applied for those personnel with identified issues such as foreign influence and foreign preference, provided the additional processes apply regardless of the citizenship or country of origin of the individual.

Imperative for Independent Intelligence Analysis

116. 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?

My military and business careers have taught me the importance of objective analysis in sound decision making. The principle of analytic integrity is essential to support both the warfighter and policy maker. If confirmed, I will fully support efforts to ensure defense intelligence analysis is objective and free from the personal biases of individual analysts or managers. I am aware of and fully support actions taken by OUSD(I&S) in light of recommendations made by the DoD Inspector General in 2018 to ensure analytic integrity. These include establishing an analytic ombudsman at each defense component that produces intelligence analysis, as well as an analysis of alternatives to evaluate differing hypotheses when applicable.

The Defense Intelligence Workforce

The USD(I&S) exercises policy oversight of the 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.

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

I believe people are the most important part of any organization. I have not yet had an opportunity to assess the size and capability of the civilian intelligence workforce. It is my impression that the Defense Intelligence and Security Enterprise is providing timely and reasoned intelligence products to the warfighters and policy makers. However, an organization must continue to adapt. In this current environment, I suspect areas of continued focus would include cyber and STEM expertise. If confirmed, I will review the future needs of the intelligence workforce and requirements of the DISE with the Under Secretary.

118. 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 military and the National Security Council staff, it is my impression that the Defense Intelligence and Security Enterprise is providing quality and timely intelligence to the war fighter and policy maker. However, as with any organization, missions evolve and adjustments to the workforce are needed. If confirmed, I will work with the Under Secretary and our intelligence leaders to assess our workforce alignment to NDS priorities, and propose such actions as may be deemed beneficial.

119. 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 been fully briefed on the candidate pools available for consideration. However, as I previously stated, I believe people are the most important part of any organization and to ensure we have the most qualified intelligence and security professionals we must persistently and aggressively seek opportunities to expand those in consideration. Where this falls short of requirements, we must work to adjust policies and procedures to address root causes.

120. What is the "time to hire" for non-executive members of the DOD civilian intelligence workforce?

I understand that the current time-to-hire an applicant within the DISE runs on average between 120 to 180 days. I believe we cannot compete for the best talent without responsive and transparent recruiting, hiring, and vetting practices, so I am eager to support current reforms to reduce hiring time where possible and seek new ones where available. I understand for all components, security clearance processing is a major factor in time-to-hire.

121. 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 provides the executive leadership for the Defense Intelligence and Security Enterprise. As DoD's executive corps, I believe the SES Executive Core Qualifications – leading change, leading people, results driven, business acumen, and building coalitions – provide a sound underlying basis for executive selections. Leadership is the most important factor for me. In the context of the intelligence mission, I believe there is a premium on a proven ability to collaborate effectively to enable impact within the integrated intelligence mission.

The Defense Intelligence Senior Level corps complements our executive core. For selection into the DISL, I would look for extraordinary personal expertise or experience in the field for which we are selecting.

122. 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 intend to use the executive performance management system within the Defense Intelligence and Security Enterprise to maintain oversight of executive and senior level performance across the Enterprise.

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

I have not yet been briefed on the content and rigor of the DISES and DISL professional development programs within DoD. However, if confirmed, I will assess the effectiveness of these programs. I believe that a talented and effective leadership cadre is critical to the success of the Defense Intelligence and Security Enterprise in delivering quality intelligence to the warfighter and policy maker.

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

I have not yet been fully briefed on the processes in place for validation of DISES and DISL requirements. However, I recognize the process of continuous evaluation of those requirements within the Enterprise as an essential mechanism to ensure the DISE is appropriately structured. Every executive wants maximum flexibility to adapt the organization to support mission success, and if confirmed will support efforts, in accordance with appropriate policies, to ensure the DISE remains adaptive.

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 senior executive.

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

I understand that the DoD civilian intelligence workforce participates fully in the IC Joint Duty program. All defense intelligence employees must have a Joint Duty assignment in order to be promoted to the senior levels. It also is my understanding that joint duty is encouraged in all Defense intelligence components as a key element of an individual's career development.

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

I believe the civilian joint duty program is an essential element of the professional development experience for members of the DoD civilian intelligence workforce. It is key that our civilian intelligence professionals understand the relationships among the members of the intelligence community, and that they build personal relationships across the IC. This joint experience supports the vital need to fully integrate the intelligence

community. Just as the military joint duty requirements from the Goldwater-Nichols Act has paid dividends for the military services, the civilian joint duty program is vital to building a more integrated, interoperable, and effective IC.

127. What are your other innovative ideas 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 the suite of current efforts to recommended specific innovative 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. Understanding the growing interdependencies with our NSIB in this environment, opportunities to gain experience in academia, and private sector entities may fulfill both of these objectives. Maximizing joint duty, the Intergovernment Personnel Act, and assignment opportunities throughout the Federal government may also increase our ability to integrate the force through professional development. Additionally, as the rate of change in workforce requirements continues to increase, supporting non-tradtional career track structures may enable both more flexibility in personal development and workforce management. If confirmed, I will pursue efforts that increase opportunities for professional development within the workforce, including the above areas of focus, and in support of critical expertise and diversity objectives.

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

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

129. 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 the flexibility to address capacity and capability requirements of the force. 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. The

Department was granted special authority under the FY 2020 Intelligence Authorization Act for limited pay authorities applicable to the National Security Agency needed to address a critical compensation shortfall in their cyber workforce. I understand this was an important action and if confirmed I will communicate any additional support needed to address DCIPS challenges, such as extending those and similar authorities to other critical skill areas within the intelligence workforce.

130. How will the enactment of Paid Parental Leave in the NDAA for FY 2020 impact the DOD civilian intelligence workforce, in your view?

I believe the Paid Parental Leave Act will provide an important benefit to the members of the intelligence workforce. I believe that offering paid parental leave will result in decreased attrition of our personnel, and will make families consider us an employer of choice in the recruitment process. If confirmed, I will work in partnership with the Under Secretary of Defense for Personnel and Readiness to ensure the appropriate policies are in place to support Defense Intelligence and Security Enterprise personnel and operations are supported through the implementation of Paid Parental Leave.

131. What are your ideas for reinvigorating long-stalled discussions with OPM for the development of an interchange agreement that would permit DISES and title 5 Senior Executives to move freely between duty positions in intelligence and non-intelligence components of all Federal departments and agencies?

I believe that, in concept, increased mobility between the DISES and title 5 SES makes sense, particularly within the Department of Defense. I feel it may be valuable to achieve seamless mobility between SES and DISES positions across the Department, and if confirmed, I will partner with the Under Secretary of Defense for Personnel and Readiness to explore ways to promote mobility, as appropriate.

132. What would be the benefits to the DOD civilian intelligence workforce of such an agreement? Are there any disadvantages to such an interchange? Please explain your answer.

I understand that one benefit to allowing free movement of DISES into the SES is in building the comprehensive capability of the federal workforce. It is always an advantage to have flexibility in how to organize your most seasoned and talented leaders. Elimination of barriers to senior mobility would provide effects similar to a vastly expanded Joint Duty arrangement. For example it could help to tear down cultural impediments to intelligence and law enforcement information sharing and facilitate interoperability of analytic tradecraft and standards, common terms of reference, and build the confidence between the IC and interagency partners required to allow the USG to fully exploit the information and expertise resident in USG. This could enhance better interagency integration, for example in support of NSPM-7. One disadvantage may be the potential loss of senior talent in critical areas if personnel management were not in

alignment with organizational objectives. If confirmed, I will continue to study the effects an interchange would have on the defense intelligence and security enterprise.

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.

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

If confirmed, I am committed to ensuring protections are afforded to DISE personnel who report fraud, waste, and abuse, or gross mismanagement, in a manner consistent with law and regulation.

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

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

Sexual Harassment

In responding to the 2018 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.

135. 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)?

If confirmed, I will exercise my oversight responsibilities for the Defense Intelligence and Security Enterprise to ensure that reports of sexual harassment or discrimination are

dealt with swiftly and in accordance with law and policy. There is no place for this conduct in the Department of Defense or Intelligence Community.

Defense Agencies

The USD(I&S) is charged to ensure the effectiveness, efficiency, economy, and performance of the Defense Agencies subject to the Under Secretary's authority, direction, and control: the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Security Agency/Central Security Service (NSA/CSS), and the National Reconnaissance Office (NRO). The USD(I&S) is accountable to the Secretary of Defense for the mission performance of each agency and for ensuring that the agencies are attentive and responsive to customer requirements, both inside and outside DOD.

136. What is your understanding of the impacts of the Defense Wide Review on the Defense Agencies under the purview of the OUSD(I&S)?

It is my understanding that the Secretary conducted the Defense Wide Review to identify resources for realignment to improve lethality and readiness in support of the NDS. Any defense intelligence and security agency resources that were affected were realigned in support of the Secretary's goals, and resources for core mission capabilities in support of the NDS were not impacted.

137. If confirmed, how should the OUSD(I&S) mitigate the potentially adverse effects of these reductions?

It is my understanding the Department is conducting in-depth analysis to identify capability gaps that exist in association with the NDS. If confirmed, I will work with defense and security agencies to help identify any potential capability gaps**.**

Space

In August 2019, DOD established U.S. Space Command (SPACECOM) and assigned it responsibility for the operational planning of DOD space missions and activities, space-related support to other combatant commands and their operational plans, and defense of space assets. The NDAA for FY 2020 authorized the establishment of the U.S. Space Force as a sixth military service, charged to undertake missions and operations in the rapidly evolving space domain.

138. 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 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 opportunities between NRO and other military space organizations to enable sharing of technology that is mutually beneficial to DoD and IC.

139. How would you deconflict taskings in the space warfighting domain across DOD with taskings 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. I foresee growth in the collection and analytical needs of the space intelligence and defense missions and, if confirmed, I will work with the functional managers on ways to increase access, agility, and responsiveness of the tasking process to best satisfy these unique intelligence requirements.

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

The key to an effective "protect and defend" strategy is the seamless execution of space defense actions, synchronized across DoD and IC platforms under a collaborative unity of effort. The National Space Defense Center is where this unified defense comes together. As adversaries increasingly threaten US freedom of action in space, the DoD and IC must continue to strengthen partnerships to maintain a competitive advantage. In crisis and in conflict, the NRO will provide support, as appropriate, to the Commander of USSPACECOM for protection of critical space assets.

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

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

The defense intelligence workforce offers a variety of capabilities to the U.S. Space Force, including intelligence support to space, technical and acquisitions expertise, and satellite operations. The Defense Intelligence Enterprise will continue to align resources and manpower to support the U.S. Space Force (USSF) establishment. While I would expect that some manpower will be realigned directly to support USSF, a federated approach will likely optimize capabilities and resources to address growing 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.

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

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

143. If confirmed, how will you guarantee that NRO has the capability and capacity to support DOD's priority space warfighting missions, while ensuring responsiveness to the needs of other NRO mission partners?

Balancing requirements and resources to support the space warfighting mission, while meeting other mission partner needs, is achieved through joint DoD and IC processes. The USD(I&S) participates in these requirements through validation, resourcing, and oversight processes. If confirmed, I will work closely with the NRO, the IC, and other senior leaders in the Department to ensure NRO mission partners' requirements receive full representation in these processes.

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

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

145. Do you perceive a need to establish an intelligence component within the newly established Space Force? Why or why not?

I believe that DoD and ODNI should ensure that the U.S. Space Force (USSF) has the intelligence necessary to accomplish its mission. Like the other military services, the USSF is a key customer of the IC and may benefit from its intelligence and counterintelligence elements being designated as an IC element at some point in the future. The DoD and IC will continue working together to ensure intelligence support to the USSF in its role to organize, train, and equip the joint force.

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.

146. 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; in accordance with applicable laws and long-standing Department and Executive Branch practice.

147. 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; in accordance with applicable laws and long-standing Department and Executive Branch practice.

148. 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; in accordance with applicable laws and long-standing Department and Executive Branch practice.

149. 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; in accordance with applicable laws and long-standing Department and Executive Branch practice.

150. 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; in accordance with applicable laws and long-standing Department and Executive Branch practice.

151. 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; in accordance with applicable laws and long-standing Department and Executive Branch practice.

152. 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; I agree to protect DoD personnel from unlawful retaliation.