D, Senate Armed Services Committee
Advance Policy Questions for Mr. Dana Deasy
Nominee for Appointment to be Department of Defense Chief Information Officer
October 21, 2019

Duties and Qualifications

Titles 10, 40, and 44 U.S. Code, establish a diversity of duties and responsibilities for the Chief Information Officer (CIO) of the Department of Defense.

1. **What is your understanding of the duties and functions of the CIO?**

The DOD CIO serves as the primary advisor to the Secretary of Defense for matters of information management, information technology, and cybersecurity, as well as critical satellite communications, navigation and timing programs, spectrum, and telecommunications. The DOD CIO is also responsible for budget certification and developing, adopting, or publishing standards for IT and cyber areas of responsibility. The Secretary of Defense has also delegated the responsibility of integrating and fielding artificial intelligence solutions across the Department of Defense.

2. **If confirmed, what if any additional duties and functions do you expect that the Secretary of Defense would prescribe for you?**

If confirmed, I do not expect that the Secretary of Defense will prescribe any additional duties. However, if confirmed, I stand ready to support the Department at the Secretary's direction.

3. **What background, experience, and expertise do you possess that qualifies you to serve as Chief Information Officer? Please include specific examples of insights from your private sector experience as a Chief Information Officer or in similar roles, as well as your service to date as the DOD Chief Information Officer.**

Although this is my first position in government, during my 38-year career I have had the opportunity to work for some of the largest, most complex companies in the world, including building and launching the space shuttles at Rockwell, the automotive industry at General Motors, my international conglomerate experience at Siemens, the oil and gas sector at British Petroleum (BP), and most recently at JP Morgan Chase in financial services. All of these positions have had one key thing in common: technology is at the heart of their success. My diverse industry experience has been an incredible asset in navigating the complex dynamics of the Department of Defense.

4. **Given your observations and experience to date as DOD Chief Information Officer, if confirmed, what innovative ideas would you consider implementing with regard to the structure and operations of the information enterprise of the Department of Defense?**

The DOD CIO is working to empower our warfighters with the interoperability, access to data, and innovative technologies needed to succeed in multi-domain operations. Cloud computing, supported with effective data management and agile software development, provides the foundation for the delivery of enterprise services to the tactical edge. This also enables the integration of AI-enhanced capabilities throughout the force. New technologies such as 5G will support ubiquitous, low-latency communications which will transform our C3 architectures. Along with the increased use of commercial systems, DOD must leverage these capabilities to advance digital modernization and maintain military advantage.

5. **What is your understanding of the respective responsibilities of the Principal Cyber Advisor and the Chief Information Officer regarding the Department's cyber activities and cybersecurity programs and architecture?**

As the DOD CIO, I am the senior DOD official responsible for all aspects of cybersecurity and information security. Through the authorities provided in the FY 2018 National Defense Authorization Act, DOD CIO also certifies cyber-related expenditures including cybersecurity, cyberspace operations, and cyber R&D. DOD CIO also serves as the chief risk executive for cybersecurity risks. The role of the Principal Cyber Advisor (PCA) is to provide authority, direction, and control of USCYBERCOM, and ensure integration of DOD activities that support cyberspace operations.

6. **Does this allocation of responsibilities need to be changed or clarified, in your view? Please explain your answer.**

At this time, I do not foresee a need to alter or clarify the responsibilities between DOD CIO and PCA. Our organizations have a very close working relationship, each working with clear understanding of our complementary roles and responsibilities.

Section 910 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2018 transferred responsibilities for data and business system research and development, acquisition, and management to the Chief Management Officer.

7. **In your view, should this assignment of responsibilities to the Chief Management Officer be retained, reversed, or addressed in some other way? Please explain your answer.**

The DOD CIO organization works well with the CMO and we collaborate closely on a number of activities including reform, data management, and oversight of business systems. I am supportive of currently proposed NDAA language that clarifies the division of responsibilities by realigning responsibility for IT oversight of business systems to the DOD CIO. Further, the Department is working to determine the most appropriate alignment of the Chief Data Officer function within DOD, in accordance with 44 U.S.C. 3520(c), and requests freedom to complete this decision and align the organization consistent with existing law and the needs of the Department.

8. **What is your understanding of the respective responsibilities of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) and the Chief Information**

Officer for the acquisition of cybersecurity, information technology, and command, control, and communications systems, including contracting and software development?

USD(A&S) is responsible for the operation, processes, and management of the Defense Acquisition System (DAS). USD(A&S) is also the DOD lead for the publication of rules in Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS). DOD CIO is responsible for the architecture, standards, and requirements for cybersecurity, information technology, and command, control, and communications systems, which must be acquired through the DAS, FAR, and DFARS processes and rules.

9. **Does this allocation of responsibilities need to be changed or clarified, in your view? Please explain your answer.**

At this time, I do not foresee a need to alter or clarify the responsibilities between DOD CIO and USD(A&S). Our organizations have a very close working relationship on issues related to software and information technology acquisition, each working with clear understanding of our complementary roles and responsibilities.

10. **What is your understanding of the respective responsibilities of the Under Secretary of Defense for Research and Engineering (USD(R&E)), the (USD(A&S)), other components of the Department of Defense, and the CIO, for the development, procurement, and use of artificial intelligence technologies?**

As outlined in the June 27, 2018 memo establishing the JAIC, the CIO is responsible for accelerating the delivery of AI-enabled capabilities, scaling the Department-wide impact of AI, and synchronizing DOD AI activities to expand Joint Force advantages. The JAIC focuses on fielding, adoption, and integration of AI at speed and at scale. My understanding is that the Under Secretary of Defense for Research and Engineering leads the development and oversight of the DOD's technology strategy, while the Under Secretary of Defense for Acquisition and Sustainment leads all matters concerning Departmental acquisition and sustainment. In this way, AI is consistent with most capability areas in which a single organization does not direct the whole arc of activities from research to sustainment. In accordance with their statutory responsibilities, the military Services are responsible for organizing, training, and equipping their respective forces. This includes AI research and development, integration into Service weapon systems, and force-wide education and training.

11. **Does this allocation of responsibilities need to be changed or clarified, in your view? Please explain your answer.**

Section 238 of the FY 2019 National Defense Authorization Act required the Department of Defense to assess its posture for AI adoption, including an assessment of existing responsibilities. I look forward to submitting this assessment to the Congress by the end of

November. I would also note that, pursuant to Section 238, the Deputy Secretary designated the Director of the JAIC as the senior official with principal responsibilities for artificial intelligence. This designation requires the JAIC Director to carry out DOD-wide tasks in the areas of governance and oversight of AI and machine learning policy, accelerating AI development and fielding, and ensuring AI's transition to operational use. We are assessing whether the current allocation of responsibilities is suitable for this new mandate and will share our initial findings with Congress.

12. **What is your understanding of the respective responsibilities of the USD(R&E), USD(A&S), and the Chief Information Officer in prioritizing research and development activities that will provide enhanced information enterprise capabilities for the future of the DOD? What are the major emerging technologies and software development practices that you believe will have the greatest effect on the success on the Department's information enterprise into the future?**

USD(R&E) has primary responsibility for advancing technology within the Department and is: working to accelerate the fielding of 5G; developing transformational cyber security capabilities; and, via DARPA, investing heavily in the future of AI. USD(A&S) leads the Department's efforts to acquire, field, and sustain critical capabilities, and has been leading important initiatives to mitigate cyber risks to our weapons systems, promote a DevSecOps framework for software development, and reform software and IT acquisition. Their success underpins my ability to deliver digital modernization to the warfighter.

13. **What is your understanding of the respective responsibilities of the Executive Committee on Electronic Warfare, the Designated Senior Official established under section 1053 of the NDAA for FY 2019, and the Chief Information Officer for the management of electronic warfare and management of electromagnetic operations, standards, and policy?**

The responsibilities of the Executive Committee on Electronic Warfare (EW EXCOM) include providing advice on electromagnetic warfare and electromagnetic spectrum operations (EMSO) investments and ensuring their coordination across the Department. As the Senior Designated Official, the Vice Chairman of the Joint Chiefs of Staff develops requirements and specific plans for addressing personnel, capability, and capacity gaps in the electronic warfare mission area. As the DOD CIO, I provide policy and oversight on matters related to electromagnetic spectrum and electromagnetic environmental effects for the DOD.

14. **Does this allocation of responsibilities need to be changed or clarified, in your view? Please explain your answer.**

Under the direction of the EW EXCOM, my team is currently assessing the current allocation of responsibilities to determine what, if any, changes need to be made to ensure effective oversight and guidance are provided for this mission. The results of this assessment should be completed by the end of the year.

Major Challenges and Opportunities

15. What do you consider to be the most significant challenges that you would face if confirmed as the Chief Information Officer?

I have experienced a number of challenges since holding this position. The most significant challenges have been: 1) establishing a top leadership culture within DOD CIO in order to develop and execute the Department's vision; 2) aligning the entire Department around executing the digital modernization to drive innovation; and 3) ensuring the mechanisms are in place to implement the Digital Modernization Strategy while setting it up for an enduring posture.

16. What steps, if any, have you already taken to address each of these challenges, and, if confirmed what additional steps will you take?

I have taken a number of key steps to address these challenges. First, I brought in a top management team to establish a solid foundation for technical competencies, leadership, and strategic vision. Second, I led the development and implementation of a Department-wide Digital Modernization Strategy that provides the roadmap towards establishing an Enterprise Cloud, field and scaling Artificial Intelligence, modernizing command, control and communications (C3), enhancing cybersecurity, advancing IT Reform, and strengthening the cyber/IT workforce. Third, I aligned key leaders across the Department towards executing the Strategy while tracking metrics and milestones to create an enduring posture. If confirmed, I will focus on continued execution of the Strategy across the Department.

17. Describe significant opportunities that, in your view, DOD has been unable to leverage, or has leveraged only in part, during the period of your service as Chief Information Officer.

In my view, the most significant opportunity that we have been unable to leverage is delivering an enterprise cloud. Although we continue to move the program forward, obstacles have prevented us to leverage the cloud at a quicker pace. Those military personnel on the front lines need cloud computing availability at the tactical edge and across all classification levels to effectively execute their mission. Further, we are still in the early days of fielding AI through the JAIC and there is more work to be done.

18. If confirmed, what specific actions will you take to ensure that DOD leverages these opportunities in a suitable and timely way?

If confirmed, I will continue to put emphasis on delivering enterprise cloud. Specifically, DOD CIO will work with key stakeholders to develop a tailored approach that will get capabilities to the warfighter while ensuring the most value to the taxpayer. DOD CIO will leverage capabilities we have in place now that align to our DOD Cloud Strategy to fill technology gaps. We will work with the Services, combatant commands, and field agencies to develop plans of action and milestones to ensure the Department continues to migrate to fit-for-purpose and general cloud infrastructure. Further, we are continuing to initiate the necessary competencies for the JAIC and are working with the Services on fielding AI solutions that address lethality.

Civilian Control of the Military

19. If confirmed, specifically what would you do to ensure that your tenure as Chief Information Officer epitomizes the fundamental requirement for civilian control of the Armed Forces embedded in the U.S. Constitution and other laws?

Civilian control of the Armed Forces is a basic tenet of America's Constitution and governance. If confirmed, I would safeguard this foundational principle by exercising the duties of leadership anticipated by this fundamental requirement. I regularly and directly engage with the Secretary and I will continue to follow the direction of the civilian leadership of the United States and ensure appropriate civilian control of the Armed Forces.

2018 National Defense Strategy

The 2018 National Defense Strategy (NDS) outlined three lines of effort to generate decisive and sustained U.S. military advantage: rebuilding military readiness to form a more lethal force, strengthening alliances and creating new partnerships, and reforming the Department's business practices and culture. At the core of each of these efforts, the NDS describes a need for innovation, flexibility, and adaptability, and the streamlining of personnel, technology, and infrastructure.

20. In the time since the 2018 NDS was promulgated, please describe what you have done to execute this strategy. Where have you experienced success? Where do you see a need for continued improvement or additional focus or resources? Please explain your answer.

The DOD Digital Modernization Strategy supports the National Defense Strategy by ensuring our warfighters are being provided with the innovative technologies required to fight and win in great power competition. I have been working to aggressively implement this Strategy by driving enterprise cloud services; advancing our efforts in Artificial Intelligence, including the establishment of the Joint AI Center; modernizing DOD command, control, and communication (C3) capabilities; and prioritizing cybersecurity in all DOD systems. While enormous progress is being made, the primary challenge is ensuring that cybersecurity and digital modernization remain as enduring priorities, as technology rapidly evolves. In regards to strengthening alliances and partnerships, I have been an active member of the FVEY forums, as well as actively engaging with other allies. I have been advocating the importance of the Digital modernization Strategy and have been encouraging them to support and adopt similar efforts. Finally, I have been actively engaged on IT reform activities and aggressively pushing opportunities for our field agencies to be more efficient on how they manage IT.

Relationships with Other Department Offices

21. As Chief Information Officer for the Department, what do you perceive to be the appropriate relationship between you and the CIOs of the Military Services, the

Joint Staff J6, and Defense Agencies?

As the DOD CIO, I am the senior DOD official responsible for all aspects of cybersecurity, including the certification of IT budgets across the Department. The Digital Modernization Strategy sets forth goals that cannot be achieved without support from the Service CIOs, the Joint Staff and other components within DOD. While their roles and responsibilities vary, they are my key partners in developing, disseminating, and monitoring cyber-related policy across the Department and we meet frequently. They serve as critical advocates within their organizations for prioritization, resourcing, and implementation activities necessary to successfully implement digital modernization. The DOD Digital Modernization Strategy sets ambitious goals that cannot be achieved without close collaboration across the Services, Joint Staff, and Defense Agencies. Additionally, I have the ability establish IT and cyber standards as required.

22. **In your experience to date as DOD Chief Information Officer, how have you ensured consistency of approach and unity of effort to strategy development, planning, policy making, and oversight, in the information enterprise across the Department of Defense? Is there anything you might do differently, if confirmed?**

Based upon the foundations of the National Defense Strategy and Digital Modernization Strategy, I have worked with partners across the Department to develop detailed strategies to advance our efforts in cloud, AI, C3 modernization, and cybersecurity. We worked with the Components to produce Capability Planning Guidance that informs Service investments in the Program Objective Memorandum (POM). Finally, via my role in certifying the IT budget, we monitor these investments throughout the Future Year Defense Program (FYDP) to ensure our priorities stay fully aligned and resourced. This process has improved over the past two years, but if confirmed, I will work to develop and promulgate this guidance to the Services earlier in their budget cycle so it can have the maximum impact.

23. **In your experience to date as DOD Chief Information Office, how have you avoided unnecessary duplication between your efforts as the Department's CIO and the CIOs for each Military Service? Is there anything you might do differently, if confirmed?**

The MILDEP CIOs are my principal partners for ensuring that our forces are organized, trained, and equipped with the modern information technology relevant to the National Defense Strategy. Each Service has organized its CIO functions differently, and I have been working closely with them as they seek to increase the prominence of this important role. I meet with the MILDEP CIOs on a weekly basis to share information and address challenges, and if confirmed I will continue to invest in our growing collaboration.

24. **In your experience to date as DOD Chief Information Officer, have you observed or experienced circumstances in which critical information enterprise responsibilities have been "dropped" or otherwise left undone? If so, please explain your answer and describe how you have rectified the situation. If confirmed, what systemic changes would you introduce to avoid this same circumstance going forward?**

Management of the DOD Information Enterprise is all about making trades. Over the past decade-plus of focus on the counter-terror fight, the Department made a number of risk decisions related to IT systems and IT in weapons systems. In many cases DOD accepted risks that seemed manageable in the asymmetric counter-terror fight, but now appear untenable as the Department considers the challenge of facing off against near-peer adversaries. The Department has accumulated considerable technical debt over the years as we deferred upgrades and delayed modernization of key systems. Some of this debt is now coming due. DOD CIO has a significant role to play and tools that can be used to drive investment decisions. One of the most effective tool is my ability to withhold certification of a budget that does not make the appropriate steps towards addressing our technical debt.

25. **What is your relationship with the USD(R&E) with respect to research, technology development, and prototyping activities to support current and next generation defense software, cybersecurity, information systems, spectrum, and networking capabilities?**

The DOD CIO organization partners with USD(R&E) in a number of areas that represent some of the most significant and pressing technical opportunities facing the Department. In general, USD(R&E) is focused earlier in the lifecycle of the technology on research, development, experimentation, and pilots. The DOD CIO focuses on fielding and integration into the enterprise. This model has proven effective for DOD in support of both Artificial Intelligence and 5G. In addition, we work closely with DARPA to advance cybersecurity technologies to transition and field them to the warfighter.

26. **What is the role of the DOD CIO vis-à-vis the Defense Digital Service and the United States Digital Service in developing and deploying software expertise and capabilities for the Department of Defense?**

DOD CIO and the Defense Digital Service (DDS) are closely aligned in many of our objectives. First among these is a shared desire to improve the way software is designed, developed, deployed, and secured across the Department. The DDS is a source of innovation inside the Department and provides perspectives that have led to cultural changes with how we approach software development. We are working to adopt and adapt both their methodology and their tools to the larger DOD environment. In addition, DDS has been a strong partner in designing and implementing next-generation network security solutions, such as zero trust networking. I engage regularly with other Federal CIOs to share insights and address common challenges through the Federal CIO Council.

Acquisition of Information Technology and Cyber Infrastructure and Capabilities

27. **NDAAs since 2015 have enacted sweeping reforms of defense acquisition organizational structures, processes, and systems, which include emphasizing shortening acquisition cycle times, diversifying acquisition approaches and mechanisms, and delegating acquisition authorities. More recent reforms have focused on digitizing the Department and promoting reliance on the "agile" development of software-intensive systems, applying methods to deliver continuous**

product improvement, at greater speeds. How have you made use of these acquisition approaches and the "agile" method of software development in your service as CIO to date?

DOD CIO is partnered closely with USD(A&S) to drive the Department to use modern methods of software development, such as agile and DevSecOps. Our shared goal is to put new software tools into warfighters hands more quickly without sacrificing cybersecurity, quality, or resilience. This is the promise of "agile," but we will need continued collaboration across the DOD to achieve these outcomes. DOD CIO is working on building the enabling enterprise infrastructure – a set of playbooks, tools, and cloud services – that will be available across the Department to facilitate agile development. Enterprise cloud will be a strong enabler toward pivoting toward agile and DevSecOps methods.

28. What are your views on the role of data and data science in supporting these information system acquisition reforms and the "agile" lifecycle?

Our objective is to treat data as a strategic asset. In so doing, we are looking to develop a data management framework that enables data scientists to conduct the data analytics and business intelligence required to support evidence-based decision making in support of acquisition reforms in the agile life cycle. By modernizing systems and reforming information system acquisitions, we are positioning the Department to utilize data as a strategic asset.

29. How have you led DOD in using these reforms and methods in its own acquisition efforts—including market research, testing and certification, and contracting vehicles—to leverage non-traditional cybersecurity and information technology performers and solutions?

The DOD CIO has played a roles in issuing policy and guidance for systems acquisition concerning data, interoperability, and cybersecurity into the acquisition efforts for information technology. In conjunction with the acquisition community, the DOD CIO continues to support the established Key Performance Parameters (KPP) that systems must address in order to achieve affirmative acquisition Milestone Decisions. Furthermore, the DOD CIO has issued guidance to perform an IT Business Case Analysis for every major IT system where courses of action must consider cybersecurity and market research as components of alternatives. Our focus on new approaches to software development, particularly in the areas of agile development and DevSecOps, is also creating new opportunity for non-traditional contractors who have often been faster to adopt and master these techniques.

30. In your view, how should the DOD information enterprise balance the acquisition and adaptation of commercially available, off-the-shelf cybersecurity, information technology and business systems with the development and acquisition of government-unique solutions? Is there a role for both approaches depending on specific mission and technical needs or is one clearly superior to the other in the context of the Department of Defense? Please explain your answer.

There is a role and requirement for both the adoption of commercial solutions and government-unique solutions. The Department's approach is to acquire commercially available, off-the-shelf solutions to the maximum extent possible. However, the Department seeks out DOD unique solutions where commercially available, off-the-shelf capabilities do not satisfy DOD mission needs.

31. **Do you see the Department of Defense as moving towards procurement of information technology- and cybersecurity-as-a-service? What are the implications for DOD's acquisition processes should this approach prove effective and efficient?**

I recognize the value of 'as-a-service' procurement, and believe that there are cases where it offers advantages in areas of information technology and cybersecurity to fulfill mission requirements. One of the key implications and considerations of 'as-a-service' procurement is the tradeoff between control and agility. On one hand, the acquirer loses control on the means by which the outcome is achieved; on the other hand, the acquirer gains currency, because the service provider is able to keep up to date with the most effective way to achieve the specified outcome. I believe that as-a-service procurements will continue to play an important role in acquisitions of IT and cybersecurity capabilities.

32. **In your view, what role should the Defense Information Systems Agency play in facilitating the development, acquisition, and sustainment of information technology and cybersecurity capabilities across the Department of Defense?**

Modern warfare will require an all-domain approach to dealing with near-peer adversaries and this will increase the importance of IT systems that operate seamlessly across geographic and organizational boundaries. As the Department looks to identify joint, enterprise solutions to common problems, DISA is postured to support the consolidation of disparate systems into broader enterprise solutions. We are currently working with DISA to advance this type of modernization in support of the reform pillar of the National Defense Strategy.

33. **How could DISA improve its performance in this regard in your view, including technology development and systems acquisition? What actions have you taken to improve DISA's performance during the period of your service as CIO? If confirmed, what steps would you take next, and why?**

I have challenged DISA to improve its performance regarding technology development and systems acquisition by eliminating legacy systems recognized as outliving their utility and focusing on innovative approaches to today's performance challenges. Since my arrival we have strengthened the top leadership of the Joint Service Provider (JSP) organization to improve support to senior leadership in the Pentagon. I placed a pause on the Joint Regional Security Stack implementation until such time the reliability meets the needs of the Department. Finally, I have reviewed and concurred on the appropriateness of the overall DISA/JFHQ-DODIN organizational construct. If confirmed, steps to be taken in the future would include working with the Services to evaluate the network operations offerings that DISA performs today against commercial offerings. This will be done to ensure we are using the most up to date, secure technology with improved service at the right competitive price. I would consult with Congress before any significant DISA service change was introduced.

34. **In your view, what role should the National Security Agency's newly established Cybersecurity Directorate play in facilitating cybersecurity market research, testing, and acquisition across the Department of Defense? What actions have you taken to collaborate with the National Security Agency to improve its performance in this role and responsiveness to DOD requirements during the period of your service as CIO? If confirmed, what "next steps" would you take to move this initiative forward, and why?**

General Nakasone has been a close partner since I joined the Department, and I am fully supportive of the formation of this new directorate. My Cybersecurity Directorate and NSA's Cybersecurity Directorate have a close working relationship on everything from operations to budget formulation. NSA's Directorate will play a vital role in the design, testing, and certification of cryptography and will continue NSA's important research, development, and acquisition of high-assurance cybersecurity infrastructure. Our frequent meetings and close partnership on key cybersecurity priorities will continue. I believe the steps that we've already taken are the appropriate ones for moving forward and do not see anything fundamentally changing, if confirmed.

35. **During the period of your service to date as the DOD CIO, what role have you played in the Protecting Critical Technology Task Force?**

The DOD CIO has been closely engaged since the creation of the Protecting Critical Technology Task Force (PCTTF). DOD CIO is a member of the PCTTF Executive Committee, and actively participate in the decisions that are brought to that forum. My Cybersecurity Directorate developed key elements of the PCTTF work plan, and continues to support ongoing efforts and deliberation, such as refining cybersecurity standards in support of ongoing FAR and DFARS regulatory efforts.

36. **What do you view as the appropriate role for the DOD Chief Information Officer in securing the defense industrial base and national security innovation base from adversary cyber threats so as to ensure the integrity and security of DOD's classified information, controlled unclassified information, and key data? If confirmed, what "next steps" would you take to move this initiative forward?**

DOD CIO, in partnership with USD(A&S), USD(R&E), and USD(I), and in support of the PCTTF, has an important role to play in securing the Defense Industrial Base (DIB) and National Security Innovation Base from cyber threats. My organization, in partnership with USD(A&S), specifies cybersecurity standards for the protection of DOD information on industry partners' systems and networks. We are leading new cybersecurity information sharing efforts with DIB partners. There are over 450 cleared defense contractors (over half of whom are companies with less than 250 employees) currently participating in this program, and we are expanding our efforts to uncleared companies. If confirmed, I plan to further expand these efforts to medium and small companies.

37. **What do you view as the appropriate role of the DOD CIO with respect to securing National Security Systems across the government? What actions have you taken to date in executing this role and mitigating system vulnerabilities, and to what effect? If confirmed, what next steps would you take to move this initiative forward, and**

why?

As the DOD CIO, I am the DOD senior official responsible for the security of National Security Systems (NSS) within DOD. As the chair of the Committee on National Security Systems, in partnership with NSA as the National Manager, DOD CIO leads interagency efforts to ensure that NSS are properly secured across the federal government. The DOD Cyber Top 10 priorities include several initiatives to strengthen NSS and I regularly engage with the Deputy Secretary to drive implementation.

38. **What do you view as the appropriate role of the DOD CIO in working to ensure that software code developed by and for the Department of Defense is vulnerability-free and produced using secure development processes? What actions have you taken to date in executing this role, and to what effect? If confirmed, what "next steps" would you take to move this initiative forward, and why?**

Software vulnerabilities and software misconfigurations cause many cybersecurity risks. As the principal DOD senior leader responsible for cybersecurity, I am working aggressively to address these through our DevSecOps initiative. This effort aligns secure software development activities with cloud standardization. This ensures that software development will be done in a secure configuration, so that the software produced will work when deployed operationally. The DevSecOps environments being fielded in DOD will also enable enforced utilization of standard software assurance tools identified by the Joint Federated Analysis Center (JFAC). If confirmed, I will continue to drive DOD implementation of DevSecOps as part of our digital modernization efforts.

Science, Technology, and Innovation

39. **U.S. superiority in key areas of innovation is decreasing or has disappeared, while our competitors are engaging in aggressive military modernization and advanced weaponry development. DOD has identified ten key areas in which investment to develop next generation operational capabilities is imperative: hypersonics; fully networked C3; directed energy; cyber; space; quantum science; artificial intelligence (AI)/machine learning; microelectronics; autonomy; and biotechnology. What do you see as the most significant challenges (e.g., technical, organizational, or cultural) to DOD's development of these key technologies?**

The most significant challenges to DOD's development and adoption of key emerging technologies, to include AI, are organizational and cultural barriers. My experience in the private sector has shown that established organizations often take a great deal of time to adopt new technology due to the sometimes difficult process of adapting and changing well-established ways of doing business. These changes are perceived as deeply disruptive and, as a result, often meet deep institutional and cultural resistance, policy and regulatory impediments, and shifting incentive structures. Additionally, we face significant challenges in adapting legacy systems, workflows, and data to cutting-edge technologies such as AI. DOD processes need to reflect the speed, agility, and iterative nature of cloud and AI-enabled capabilities. For example, we must adapt our security accreditation and information assurance approaches to allow continuous integration and continuous delivery of AI-enabled capabilities. We must also have flexibly in our out-year budgets to continue investing in the most promising applications.

40. Are the Department's investments in these technologies appropriately focused, integrated, and synchronized across all Military Departments and Agencies?

With the Digital Modernization Strategy, the Department is committed to properly focusing, integrating, and synchronizing key technology areas in cybersecurity, artificial intelligence, cloud, and command, control, and communications. This strategy complements USD (R&E)'s long-term investments in AI that will enhance the foundation of U.S. defense capabilities relative to Russia and China. The Digital Modernization Strategy allows the Department to synchronize these technologies across the military departments and agencies. Additionally, with Budget Certification authorities, I will ensure our information technology and cyberspace activities budgets are sufficient to improve our business platforms and improve Joint warfighting. One of the JAIC's core responsibilities, in coordination with USD (R&E), is to focus, integrate, and synchronize AI activities across the Department. As necessary, I will seek your support for legislative changes to provide the requisite authorities associated with effectively executing these responsibilities.

41. In addition to the technologies identified in the 2018 NDS, are there other technology areas in which you believe DOD must invest to ensure that the United States maintains its technological superiority in the long-term?

The NDS emphasizes the broader need for digital modernization and superior information technology, as reflected by the Digital Moderation Strategy's pillars of cloud, AI, C3, and cyber. 5G and advanced spectrum capabilities will be critical battlefield enablers for advanced communications, and therefore are areas of growing investment for the Department. Quantum computing, though still nascent, along with other models of advanced computing and microelectronics, will also be critical to maintaining technological superiority in the future. DOD must also be adept at leveraging commercial practices and new ways of operating to fully harness these technologies for battlefield advantage.

42. What efforts is DOD making to identify new technologies developed commercially by the private sector and apply them to national security and warfighter purposes?

DOD CIO has established partnerships with industry including large established technology firms and small startups. Furthermore, we leverage the venture capital community to identify emerging technologies. Examples of areas where we have created partnerships include cloud computing, fielding new AI and 5G capabilities, solutions for spectrum sharing and commercial satellite communications, and defeating advanced cyber threats.

Budget Review and Standards-Setting Authority

43. Section 909 of the NDAA for FY 2018 empowered the DOD Chief Information Officer to exercise budget review and certification authority to ensure that the budgets of Department of Defense components with responsibilities associated with any activity specified in section 142(b)(1) of title 10, U. S. Code, are adequate for such activities. In your service to date as DOD Chief Information Officer, how have

you used this budget review and certification authority to shape the modernization and prioritization of cybersecurity and information technology infrastructure? If confirmed, to what investments and objectives do you envision this authority best could be put to use going forward?

The DOD CIO budget review and certification authority provides a critical avenue for a more strategic and methodical approach to prioritize resources toward capability requirements in order to further the National Defense Strategy. I used these authorities for the first time in the FY 2020 budget to start shaping spend towards the digital modernization program. If confirmed, I will use this authority to ensure that future year defense program invest in capabilities that support the Digital Modernization Strategy and NDS.

44. In response to your exercise of budget review and certification authority under section 909, have Department of Defense components adjusted their budget proposals to support your priorities? If so, what kind of adjustments have been made, with regard to what sort of systems and programs?

The DOD CIO successfully completed the first budget review and determination since the enactment of section 909, certifying that the DOD FY 2020 PB adequately resourced the required capabilities within the DOD CIO areas of responsibility. I used the budget certification authority to ensure that the Department is making solid progress toward increasing the focus and priority toward Digital Modernization efforts, and that investments were targeted at selected priorities. For example, the FY 2020 President's Budget (PB) significantly increased resources for artificial intelligence and cybersecurity programs across DOD Components. Programs and efforts with increased FY 2020 resources included:

- $268M in additional funds for the JAIC.
- $242M in additional funding to support cybersecurity efforts.
- An additional $7M to address the DOD-wide shortfall for critical cyber workforce talent through the management of the Cyber Excepted Service.

45. What actions have you taken, or would you propose to take, if confirmed, to ensure that directives, policies, and standards originating from your office, are adopted and implemented consistently and rapidly throughout the Department? If confirmed, by what specific means and methods would you exercise your oversight responsibilities to assess other Components' adherence to your directives?

DOD CIO works closely with the Military Department CIOs to ensure they understand and are in fact complying with policies and guidance that have been issued. Additionally, DOD CIO participates in decision forums led by the offices USD (A&S), the Chief Management Officer, and DOD Comptroller to ensure that Component's programs and investments are in compliance.

I have regular meetings with the Deputy Secretary of Defense and advise him on progress towards implementing the Digital Modernization Strategy.

<u>Cybersecurity Architecture</u>

46. In your view, what are the major challenges facing the Department of Defense as regards its cybersecurity programs and capabilities?

DOD systems and networks are high-priority targets for the most sophisticated threat actors in the world, so DOD requires the best defenses. Our adversaries are constantly evolving their tradecraft, i.e. finding new ways to penetrate DOD's defenses. We must recognize that we will be continually updating our security posture. This will require an ongoing investment in refresh of our technology environment. However, we must carefully prioritize investments. We must leverage new capabilities to make it more expensive to attack and less difficult to defend our networks.

47. In your view, how effective are the Department's cybersecurity programs, capabilities, and common infrastructure—at the perimeter, at the network layer, and across endpoints—in detecting and defeating advanced persistent threats in real-time?

The Department's cybersecurity programs, capabilities, and common infrastructure are most advanced at our perimeter and network layers, including both filtering and cryptographic capabilities. We believe they are generally effective against all but the most sophisticated threats. The end-point and data-centric approaches, which lay the foundations for our zero-trust approach, were requested in the President's FY 2020 budget. These hold the promise of significantly strengthening our defensive posture.

48. Which of the Department's programs, capabilities, or common infrastructure are pressingly obsolete or ineffective, in your view? What programs, capabilities, or common infrastructure must the Department of Defense procure and prioritize to improve its cybersecurity posture and resiliency in the face of advanced persistent threats? How would you address the gaps between DOD's legacy systems and your objective programs, capabilities, and infrastructure?

The DOD's enterprise networking and computing infrastructure continually requires modernization, which is currently underway. There are also increasing opportunities to shift to commercial service providers, such as enterprise cloud and commercial cybersecurity capabilities. The real challenge is legacy systems tied to fragile and outdated technologies are difficult to modernize. The implementation of the Digital Modernization Strategy has created an environment where new systems are able to be built cyber secure from the ground up (e.g. DevSecOps and Zero Trust). For systems that cannot yet be replaced, we have a forum chaired by the Deputy Secretary of Defense where we track remediation of these cybersecurity risks.

49. In your view, how adept and effective are the Department's cybersecurity and information technology operators, including its cybersecurity service providers, in consistently detecting and defeating advanced persistent threats in real-time? Do these personnel and their systems have substantial visibility into DOD networks and across their endpoints?

I am encouraged by the maturation and sophistication of USCYBERCOM/JFHQ DODIN, the Service cyber components, DISA Global Operations Command, and the DOD Cybersecurity Service Providers, but believe that there is significant room for improvement when it comes to taking advantage of automation to remove labor intensive activities. This has been a point of emphasis for me over the past year, and DoD has already seen significant improvements in the real-time visibility of our endpoints to compliment the substantial visibility our operators have into DoD networks. We are continuing to drive automation into other facets of our defenses, to present operators an integrated real-time picture through which they will be able to better defeat advanced persistent threats.

50. **Are Joint Forces Headquarters-Department of Defense Information Networks and Defense Information Systems Agency Global Operations Command sufficiently resourced, manned, and equipped to serve as operational command and control hubs for the Department of Defense's cybersecurity? In your assessment, to what extent do they link together the Department of Defense's cybersecurity operators and capabilities at the perimeter, at the network layer, and across endpoints? In your assessment, to what extent do they provide real-time direction and orchestration of cybersecurity operations? In your view, do they have substantial visibility into Department of Defense Components' networks and endpoints? In the period of your service to date as CIO, what management actions, policies, acquisition efforts, and timelines have you undertaken or established to address the challenges or deficiencies in the performance of these entities? If confirmed, what would you see as the next logical steps going forward?**

General Nakasone and I partner closely regarding resourcing and equipping JFHQ DoDIN and DISA Global Operations Command (DGOC). JFHQ DODIN has reached Full Operational Capability, and I do believe that it provides an effective integration of DoD cybersecurity operators across the full spectrum of our defensive capabilities for their core missions. With that said, I do believe continuous evolution of their capacity is required given the continually changing threat landscape. JFHQ DoDIN has proven their ability to provide direction and orchestration across DoD Components. Likewise, DGOC has proven to be an effective operator of DISA enterprise solutions, to include the network, perimeter defenses, and endpoint software. As with many DoD missions, JFHQ DoDIN and DGOC would both benefit from additional resources, but network defense against our adversaries requires a robust defense at all layers of our defensive structure - from our enterprise capabilities provided by JFHQ DoDIN and DGOC, down to the contributions of the Service Components. General Nakasone and I will continue to drive improvements into these organizations, and I will use my budget certification authority to ensure that the full spectrum of DoD cyber operations is appropriately resourced.

Information Technology, Networking, and Cloud

51. **In your view, what are the major challenges facing the Department of Defense as it relates to its information technology, networking, and utilization of cloud technology?**

The DOD Digital Modernization Strategy seeks to address many of the major technology challenges faced by the Department. These challenges include the fact we currently have numerous clouds and networks that require much greater integration and provisioning of enterprise tools. We have accrued technical debt by delaying the modernization of many key C3 systems that are now obsolete or require recapitalization. We have given insufficient attention to the cybersecurity of all DOD systems, and thus require sustained investments in mitigating these risk and doing so continuously throughout a system's lifecycle. Finally, we must become more adept at rapidly adapting, certifying, and fielding new technologies to the warfighter.

52. How is the Department using microsegmentation and software defined networking to improve networking performance and cybersecurity? What prototyping and acquisition efforts are underway to incorporate microsegmentation and software defined networking into the Department's computing and network architecture?

The Department developed and is implementing an approach to rapidly deploy advanced commercial networking capabilities, including software-defined networking (SDN), bandwidth on demand, and aggregated cloud access gateways. Presently, DISA is piloting SDN at various sites within the DISN core and we will leverage the findings of these pilots in order to expand use of SDN through ongoing technology refresh across the DODIN. We are currently developing micro segmentation as part of our future zero-trust architecture, and exploring different technical and process actions. USCYBERCOM, NSA, and DISA are currently experimenting with overall zero-trust concepts, to include microsegmentation.

53. In the period of your service to date as CIO, what management actions, policies, acquisition efforts, and timelines have you undertaken or established to address the challenges or deficiencies in these domains? If confirmed, what would you see as the next logical step going forward?

DOD CIO has provided guidance and associated objectives to the Department via the Digital Modernization Strategy, with pilot efforts guiding the establishment of timelines. DOD CIO has also developed specific strategies for Cloud, Artificial Intelligence, and Cyber to complement the Modernization Strategy. These strategies inform our planning guidance to the Military Departments and drive the development of Enterprise Services designed to support key functions for all of DOD. If confirmed, my focus in the next year will be on execution against these strategies. Major initiatives including the JAIC, the Enterprise Cloud initiative, our network optimization program, and a defense-wide set of collaboration tools are nearing a transition from planning and acquisition to delivery and I will be focused on ensuring we deliver for the warfighter.

54. What specific role have you played in the development of and current execution of the JEDI initiative?

Although the development of the JEDI Cloud initiative was underway, my role included bringing a private sector perspective on how best to ensure commercial parity. Though I was not directly involved in the review or evaluation of the proposals, I have guided the development of the enterprise cloud strategy and adoption of best practices. An important role I've played has been maintaining a constant dialogue between Congress and my office on the development and progress of the JEDI Cloud effort. I have also been the primary advisor to the Secretary and the Deputy Secretary.

55. What specific role have you played in the development and current execution of the

Defense Enterprise Office Solution initiative?

My specific role with the DEOS initiative was to ensure the program met the priorities within the NDS and was aligned to the Department's Digital Modernization Strategy. I have been involved in an oversight role throughout the process. I participated in DEOS reviews to understand how the requirements were being developed. I took the decision to work with GSA and the Federal CIO for the acquisition. Finally, I have advocated for the adoption of DEOS across the Department.

56. DOD's cloud strategy emphasizes diversity of initiatives and performers, balanced with the need for niche capabilities, as well as commercial solutions. Given this strategy, what do you see as the benefits of maintaining the Joint Enterprise Defense Infrastructure (JEDI), the Defense Enterprise Office Solution, MilCloud 2.0, and distinct fit-for-purpose clouds?

As no single solution is capable of satisfying the diverse needs of the Department's mission set, the DOD cloud environment will be a multi-vendor, multi-cloud environment. The DOD Cloud Strategy established the DOD Enterprise Cloud Environment to bring structure to the Department's approach to cloud. JEDI, DEOS, MilCloud 2.0, and other cloud offerings each fulfill needs within the Strategy and complement one another to provide a full set of services to the DOD. These initial cloud offerings are the first step in realizing a DOD cloud ecosystem supporting the Warfighter and other critical functions across the Department.

57. You have stated that DOD intends to make additional awards within a few years at most to establish additional commercial general purpose cloud infrastructures, using the initial JEDI award to "learn" how to manage a commercial cloud acquisition and to migrate and adapt data and applications from legacy environments to the cloud. What timelines have you established for bringing on additional commercial cloud providers?

As the Department becomes more mature in its approach to maximizing the value and potential of cloud computing, we will want to bring additional general purpose providers into the defense environment. We plan to look at the feasibility and utility of an additional contract for unclassified services. While we want to move quickly, we also need to ensure that the lessons learned from the JEDI acquisition and implementation can be incorporated into future efforts.

58. If confirmed, what timelines would you establish for the movement of DOD Components' data and networking functions to enterprise clouds?

While a specific timetable has not been set, the Department is moving to aggressively adopt cloud-based solutions and drive digital modernization. Our initial goal will be to ensure all new software development efforts will be built from the ground up to be cloud enabled. For legacy systems, the transition to cloud will depend on the long term use of the application, the migration cost, and the technical difficulty of migration. Based on my commercial experience, the movement of legacy systems to the cloud will rely heavily on a business case analysis.

59. In your view, is there value in expediting the movement of DOD Components' data and networking functions to enterprise clouds? If so, specifically what would you do to expedite this transition across the enterprise?

The migration to enterprise cloud is essential to ensuring we can seamlessly share data to the tactical edge, deliver new AI-enabled capabilities, and support the joint concepts for all-domain warfighting. To expedite this transition, the first step is completion of source selection for the cloud contract. With the contract in place, we need to clear a pathway to the cloud by updating rules and guidance for efficient provisioning and use of cloud services, updating security standards for the modern environment, and streamlining outdated processes that have slowed adoption. We will also transition to new software development practices (e.g. agile development) to fully harness the benefits of working in a cloud environment. Implemented correctly, the cloud transition will allow us to deliver more capability to warfighters faster while simultaneously improving our cyber posture.

60. If confirmed, what metrics would you establish at each stage of cloud migration to evaluate whether expected performance and analytic gains have been attained?

The initial objective is cloud adoption, which will set the foundation for building performance and analytic gains. Key metrics include cloud investment, where we should see significant growth; time to migration to ensure our processes are not hindering adoption; and migration costs to facilitate appropriate investment for future applications and systems residing in the cloud environment. In addition to measuring cloud adoption itself, we will also measure the percentage of new software applications developed using agile processes. If confirmed, I will seek to develop additional metrics to measure the effectiveness of cloud solutions supporting warfighters at the tactical edge.

61. If confirmed, what measures will you employ across the Department to ensure that: cloud data are, as appropriate, discoverable; cloud service providers' analytical and business tools are utilized; and networking and cybersecurity performance are improved?

Under my leadership, the DOD CIO is reviewing and updating Department policy and implementation guidance related to cloud computing. Our updated guidance is incorporating years of lessons learned from industry, other government agencies, and the DOD's own experience. We will use this review to set new standards ensuring the appropriate discovery of data and update procedures for ensuring systems and data are secure in the cloud. We are also developing implementation guidance to assist DOD components in taking full advantage of the tools and data provided directly by cloud service providers. Leveraging our budget certification authorities, we will encourage component adoption of best practices for ensuring cloud security, performance, and cost effectiveness.

62. What is the status of the Secretary of Defense review of the ongoing JEDI cloud computing program?

Shortly after being confirmed, Secretary Esper committed to a full review of the JEDI program in response to input he received from many quarters, including direct requests from several members of Congress. Given the high level of interest in the program, the Secretary wanted to ensure he understood the nature of the acquisition, the role of JEDI within the larger strategy, and the process the Department followed in executing the source selection. Recently, out of an abundance of caution, the Secretary formally recused himself from any decisions related to the JEDI source selection itself. The Deputy Secretary of Defense is now responsible for determining the way forward on JEDI.

Artificial Intelligence

63. In your view, what are the major challenges facing the Department of Defense as it relates to its artificial intelligence-related programs?

The Department of Defense faces four major challenges as related to its AI programs: talent, data, culture, and budgeting. AI expertise is in extremely high demand in the commercial sector. Private companies offer pay, benefits, and work environments that, in many cases, are perceived as more enticing that what the Department of Defense currently offers. Second, AI capabilities, especially machine learning applications, require vast amounts of high-quality data. I am committed to working with the Joint Staff, the Services, and other OSD components to strengthen our data management policies and help set conditions for data to be shared widely across organizations. Third, DOD faces a cultural challenge to AI adoption. This includes modernizing legacy security accreditation and information assurance processes to allow continuous integration and continuous delivery of AI-enabled capabilities. Finally, AI is a highly iterative learning process, centered on rapidly-emerging technologies. As such, the Department requires more flexibility in budget planning beyond a near-term horizon.

64. From your perspective, would DOD be best served by creating its own machine learning and artificial intelligence algorithms and software, buying existing technologies, contracting for the production of such technologies, or some combination of these?

In accordance with Congressional direction, we abide by the principle of ‘commercial first’. It is difficult for DOD to keep up with the pace of technological change in the commercial AI industry. And in many cases, commercial solutions exist for most DOD problems. Because of the diversity of our missions and complex operating environments, however, there is no single AI solution to the Department’s AI problems. The right acquisition and development approach depends upon the nature the challenge. There are benefits to each of the three approaches, and we are pursuing a combination of them for the diverse mission areas of the Department’s AI portfolio.

65. In the context of your service to date as DOD CIO, how have you led the Department in using machine learning and advanced statistical methods to improve its business, maintenance, and management practices? What demonstrable improvements have resulted from these efforts? If confirmed, what you would envision as the next steps in this process?

The JAIC currently has several initiatives that make extensive use of machine learning underway and several others that are in advanced planning stages. For example, the JAIC's Predictive

Maintenance National Mission Initiative (NMI) has multiple lines of effort underway that use machine learning and advanced statistics to improve vehicle readiness and reduce maintenance costs. One of these lines of effort involves predicting a certain failure mode in the H-60 helicopter engines. Initial results from Special Operations Command (SOCOM) have been promising. The JAIC's Intelligence Business Automation NMI is seeking to use AI capabilities to improve the productivity and efficiency of DOD management and organizational functions; in one of our first projects, the DOD's Office of the Chief Management Officer (OCMO) estimates that DOD use of a single JAIC-designed custom-built capability already in use will save tens of thousands of hours of staff work checking and re-checking certain DOD forms for compliance. These efforts are just a small example of AI's potential. I will continue to work closely with the CMO, military Services, Joint Staff, and OSD Components to find opportunities to use AI/ML to improve the efficiency and effectiveness of back-office functions across the Department.

66. Should the Department fund academic, small business, and government lab research in artificial intelligence to support defense missions and the development of new AI-enabled systems and technologies?

The White House Executive Order on Maintaining American Leadership in Artificial Intelligence emphasizes the importance of driving technological breakthroughs in AI across the Federal Government, industry, and academia to promote scientific discovery, economic competitiveness, and national security. The DOD contribution to this whole-of-government approach includes fostering partnerships with the National Security Innovation Base in order to maintain U.S. technological superiority against peer competitors, and to help ensure we make rapid progress in our Digital Modernization Strategy. The Department should leverage its full-range of tools to access cutting-edge AI technologies and associated ecosystems in support of defense missions. This AI ecosystem includes academic organizations, small businesses, government labs, FFRDCs/UARCs, and the venture capital market in addition to some of the world's biggest data companies.

67. How can the Department of Defense shape the direction of commercial artificial intelligence research and development to incentivize the production of battlefield-relevant technology, as well as better data analytic tools?

The Department, in partnership with Congress, can shape the direction of commercial AI R&D and product development primarily by sustaining financial investments in commercially-procured AI capabilities. Most commercial AI capabilities today are relevant to DOD missions, although generally they must be trained against DOD data and adapted to DOD’s unique operational environments. The JAIC brings critical mass and focused resourcing that allows the Department to incentivize the commercial sector to produce battlefield-relevant technologies and increase the capacity and robustness of the commercial AI ecosystem. The JAIC and other DOD Components have begun to influence the commercial AI ecosystem through establishing and partnering on large-scale AI projects.

68. Where and how is the Department of Defense developing the operating concepts, plans, and capabilities relevant to future artificial intelligence battlefield systems?

Along with the National Defense Strategy and DOD AI Strategy, the guiding conceptual document for artificial intelligence is the Joint Concept for Operating in the Information

Environment (JCIE) released in 2018. The central idea of this concept is to broaden the informational aspects of military activities to include how artificial intelligence increases the speed, precision, and agility of decision makers. The Joint Staff is also developing a plan on Joint Information Advantage based upon the JCIE that incorporates artificial intelligence capabilities on the future battlefield. The JAIC is already working with the Joint Staff and Project Maven on development of new warfighting operating concepts based on emerging technologies such as cloud, 5G, AI, and eventually quantum computing. This includes using experimentation, war gaming, exercises, and modeling and simulation to evaluate and refine these operating concepts.

69. What structures, processes, and policies are needed in your view to ensure the ethical and safe application of AI technology to the warfighting missions of the Defense Department?

The Department of Defense is committed to the safe, ethical, and responsible application of AI technology to its warfighting missions. The Department has faced many periods of technology transformation, and our established structures, policies, and processes have an enduring and beneficial relevance for AI. We have a robust culture of test, evaluation, validation, and verification. The JAIC is working with the military Services, Joint Staff, OSD components, combatant commands, and the intelligence community to establish policies and processes to ensure all AI-enabled capabilities developed by DOD are rigorously validated. Second, the Department prioritizes high-quality training and realistic exercises to ensure our service members are familiar with and fully proficient in the operation of any new system they are expected to use. The JAIC also serves as a Center of Excellence for capturing and promulgating valuable lessons learned as AI-enabled capabilities are fielded. Finally, the Department has a culture of legal, responsible, and disciplined use of its capabilities, including AI. We are engaging extensively with partners in academia, industry, and international organizations to develop and codify principles and practices for safe and ethical use of AI-enabled systems.

70. What steps should the Department of Defense be taking with international partners and the commercial sector to develop standards and norms for the ethical and safe application of AI technologies?

The DoD AI Strategy prioritizes leadership in applying military ethics to this technology. This remains central to engagements with international partners and the commercial sector. We are working continuously with allies and partners to strengthen interoperability and readiness, which includes advocating for the safe and ethical adoption of emerging technologies such as AI. The JAIC is also a member of both national and international standards bodies addressing AI.

Electromagnetic Spectrum Policy and Operations

71. In your view, what are the major challenges facing the Department of Defense as pertains to its electromagnetic spectrum operations programs?

The major challenges are modernizing the systems, processes, and people of the EMS enterprise into an integrated infrastructure. This includes a modern EMS architecture, joint spectrum data repository, electromagnetic battle management systems, EMS operation centers, and multi-domain cloud capabilities necessary for successful networking. Finally, we must continue to invest in a trained and ready EMS workforce capable of conducting EMS operations against near-peer adversaries.

72. **What is your assessment of DOD electromagnetic spectrum operations capabilities, as compared to the offensive and defensive capabilities of our adversaries?**

Our advantage in EMS operations is being eroded and requires greater investment, including the incorporation of advanced spectrum technologies. We have begun addressing these deficiencies as part of our digital modernization efforts, and must ensure we continue to prioritize EMS capabilities needed for high-end conflict.

73. **If confirmed, what would be your plan for improving DOD electromagnetic spectrum operations programs in the short- and long-term?**

DOD needs to fund an expanded EMS enterprise portfolio. In the long term, DOD needs to develop a set of military and civilian EMS professionals who can harness cloud, cyber, and artificial intelligence to support electromagnetic spectrum operations.

74. **What are your views regarding the potential sharing of spectrum for both federal and non-federal bands?**

Spectrum sharing is a viable and feasible way to keep pace with technological advancement in areas such as 5G and growing spectrum demands from both commercial and national security interests. National security missions require access to a wide range of spectrum bands, regardless of allocation. Reallocation of spectrum based solely on relocating out of a band is unsustainable. As Dynamic Spectrum Sharing technology continues to advance, bi-directional spectrum sharing is a viable alternative to meet everyone's needs. Additionally, DOD needs to "fight through" contested and congested electromagnetic environments. The same technologies that enable DOD to share spectrum domestically provide us with strategic advantages on the battlefield.

75. **What is your assessment of the current assignment of responsibilities and the management structure in the Department of Defense pertaining to electronic warfare and electromagnetic spectrum operations, as compared to the threats that DOD faces and the challenges you perceive?**

Under the direction of the EW EXCOM, my team is currently assessing the allocation of responsibilities to determine what, if any, expanded responsibilities are necessary to ensure effective oversight and guidance are provided for these missions. The results of this assessment should be complete by the end of the year.

<u>Positioning, Navigation, and Timing</u>

76. **In your view, what are the major challenges facing the Department of Defense as pertains to its positioning, navigation, and timing programs and capabilities?**

Immediate challenges for performing the PNT mission include modernizing the GPS command and control architecture, enabling use of the Military-code broadcast, and improving cybersecurity for mission critical systems. Additionally, we are working with the Services to ensure we have various alternatives to provide assured PNT for military systems in a contested-environment.

77. **If confirmed, how would you focus the Department on addressing each of these challenges, and on what timeline?**

If confirmed, I will continue addressing these challenges through my role as the Secretariat of the PNT Oversight Council, which is co-chaired by USD(A&S) and the Vice Chairman of the Joint Chiefs of Staff. Subordinate to the Council is its Executive Management Board (EMB), which I chair, and a series of Working Groups addressing all elements of PNT. This body, established by Congress, provides an effective means to prioritize and coordinate investments needed for PNT modernization. Additionally, I'm also able to shape PNT investments by providing annual capability planning guidance to the Department.

78. **The Committee is concerned about the dependence of the Department and indeed the country as a whole on the Global Positioning System (GPS) given the existing and anticipated threats to the system. Upgrades to GPS and user equipment are being acquired, but the lag-time is significant and concerns persist about reliance on a single source. What are your views on the need for reliable additional near-term and far-term augmentations to GPS? Is the Department adequately resourcing these needs, in your view?**

DOD CIO agrees with the need to invest in hardening and upgrading GPS and well as developing complementary systems. The direction regarding the needed investments are reflected in the capability planning guidance I provide annually to the Department. No single PNT alternative can completely replace GPS or meet the disparate needs across the Joint Force. In close collaboration with the Services, we have published a DOD PNT Strategy to guide the development of a resilient and balanced portfolio of capabilities. This will require continued investment across the FYDP to ensure successful execution of the DOD PNT Strategy.

Command, Control, and Communications

79. **In your view, what are the major challenges facing the Department of Defense as pertains to its command, control, and communications (C3) programs and capabilities?**

Modernization of our existing C3 systems is critical to maintaining our military advantage. Today we have adversaries that have developed tactics and techniques to degrade, deny, disconnect, and spoof our C3 systems. Furthermore, our legacy C3 systems have been built in compartments not well suited for multi-domain operations. We recognize future conflict with near peer adversaries will require us to have a secure, integrated, and interoperable C3 architecture.

80. **What is your assessment of the Department of Defense's C3 capabilities and resiliency in the face of near peer adversaries?**

Our advantage in C3 capabilities is being eroded and requires greater investment. We have begun addressing these deficiencies as part of our digital modernization efforts and must ensure we continue to prioritize C3 capabilities and resiliency needed for high-end conflict.

81. There has been much discussion about the importance of networking and connecting warfighting capabilities across air, land, and sea platforms.

Yes, networking and connecting warfighting capabilities across air, land, and sea platforms is the concept behind Joint All Domain Command and Control (JADC2). To meet this need, the Department must design, develop, deploy, and operate integrated capabilities that allow leaders and their assigned forces to have visibility of and easy access to information in order to quickly grasp a situation and effectively support a commander's intent and the elements of mission command.

82. What is DOD doing to make machine-to-machine command and control, across multiple domains, a reality?

The DOD has a number of ongoing efforts to address machine-to-machine C2 across multiple domains. USD(R&E) is developing a Universal C2 Architecture; the Joint Staff is leading exercises and experimentation efforts for JADC2; and collectively the Department is developing common data standards and Advanced Programming Interfaces (APIs). Additionally, the Department recognizes that one of the key requirements for achieving machine-to-machine C2 is establishing enterprise cloud capabilities at the tactical edge. Other capabilities being developed by the Joint Artificial Intelligence Center (JAIC) will help enable machine-to-machine learning. Finally, 5G has the potential to become the communication fabric that supports low latency machine-to-machine command and control.

83. Has DOD developed and refined the joint operational concepts that will govern this integrated fight?

The Joint Staff is continuing to develop new joint operational concepts for future conflict. We support the Joint Staff by developing the architectures, interoperability guidance, and security policies that establish the framework for the operational employment for our communications systems in support of Joint, Allied, and Coalition operations.

84. What is being done to ensure that airborne data links are resilient against peer competitors and interoperable—across all Military Services' platforms?

Tactical Data Links (TDLs) are a critical technology that is relied upon by the Joint Force, our allies, and coalition partners. The Department has three lines of effort to ensure that airborne data links are resilient. First, advocating that Services expeditiously close identified gaps by rapidly fielding the Multifunctional Information Distribution System (MIDS) Program of Record for Link 16. Second, identifying legacy TDLs that are vulnerable or require replacement. Finally, accelerating the implementation of advanced capabilities to increase the resiliency, robustness, and capacity of DOD tactical networks.

85. If confirmed, specifically what would you do to facilitate development and implementation of (multi-domain C2) MDC2 concepts?

If confirmed, DOD CIO will continue the Department's transition to enterprise cloud-based solutions in order to provide joint situational awareness for future command and control systems. DOD CIO will focus on implementing information-sharing standards to develop new system interfaces in order to improve interoperability, operational agility, and set the conditions for improved machine-to-machine transactions. Further work is required to ensure that information flows seamlessly across security boundaries as required.

86. How do you differentiate the role of the CIO with regard to warfighting networks that provide command and control of our armed forces at their platforms in an operational context, as compared to the CIO's role with regard to infrastructure and networks that traditionally would be regarded as administrative or otherwise non-warfighting in nature? Does your authority extend to warfighting networks and systems in the Department? Is the CIO perceived as an official with a fundamental role in the warfighting infrastructure of the Department?

There is no differentiation in my role for warfighting and administrative networks as codified in DODD 5144.01. My PSA responsibilities for information technology include warfighting networks. Therefore, the DOD CIO is recognized as having a fundamental role in the warfighting infrastructure of the Department.

87. Please describe your view of the CIO's role with respect to overseeing the cryptographic accounts at the National Security Agency (NSA) and recent efforts with respect to building new or upgrading facilities and infrastructure at the NSA for cryptographic key and management infrastructure across the DOD as well as the development and distribution of nuclear command and control products?

Modernization of all DOD cryptographic systems is vital to the security of our information and the protection of our forces, and has been a top priority for me. Through the DOD CIO's budget certification authority, I am able to provide effective oversight of NSA's budget for these programs and I support increased investment. I also work closely with the Services, Intelligence Community, and COCOMS to address current cyber and cryptographic vulnerabilities. I also have an effective partnership with USSTRATCOM regarding the security and protection of nuclear command, control, and communications systems. We continue to closely monitor any potential vulnerability in the security of these critical capabilities.

<u>Information Technology Workforce and the Cyber Excepted Service</u>

88. The Chief Information Officer serves as the functional community manager for 18 civilian occupational specialties, which account for approximately 52,000 civilian employees. Additionally, the CIO is one of the chairs of the Cyber Workforce Management Board, which oversees the management of the entire Department of Defense military and civilian cyber workforce. These are critical roles as the Department evolves its employment practices to attract and retain personnel with highly valuable information technology and cyber-related skillsets. As you shape and guide the Department's cyber workforce, how do you determine whether a certain position should be filled by military, civilian, or contractor personnel?

DOD maintains a total force management approach to provide qualified civilian and military personnel to fill authorized positions, augmented where appropriate by contractor support. To determine if a position should be contracted out, we first consider whether it is inherently governmental work. If not, DOD contracts for the support. Civilian and military personnel assigned to perform the Department's cyber mission must meet the qualification standards which consist of a combination of education, training, certification, and experience. This program helps to ensure we have the most qualified cyber workforce and that they are provided with continuous professional development.

89. **Each Military Department and DOD Component is competing for the same set of skilled and experienced employees, who are highly skilled and experienced in cyber and information technology. How does the Cyber Workforce Management Board de-conflict and prioritize personnel requirements across the Department to ensure the strategic allocation of manpower to the highest priority needs?**

The CWMB is a decision body that regularly reviews issues, identifies standards, sets requirements, and makes recommendations to the appropriate implementation authorities across the Department. It also provides guidance for the overall development of the cyber workforce and reciprocity across Components.

90. **Of the approximate 52,000 civilian employees under the DOD CIO's purview, how many should be included in the Cyber Excepted Service, in your view?**

I am supportive of our initial prioritization of billets for CES migration within Service cyber components, DOD CIO, CYBERCOM, and DISA, totaling about 15,000 eligible personnel. We will reassess this allocation as the program is built out.

The Cyber Excepted Service was authorized in the FY16 NDAA, yet implementation still is not complete.

91. **In your view, what have been the biggest obstacles to the full implementation and expansion of the Cyber Excepted Service? If confirmed, specifically what would you do to overcome these obstacles going forward?**

We have made great strides in the implementation of the Cyber Excepted Service (CES). In the past, we have struggled to put appropriate focus and priority on the CES program, and had not built elements into the program that the Services required to be able to effectively use the authority. To resolve this, I have added resources to my team to accelerate buildout of the program, and have reprioritized work to ensure that we are building out the most important aspects of the program first. As a result of these efforts, the US Navy and US Marine Corps have joined CYBERCOM, DISA, DOD CIO in converting their cyber components to CES. In addition, the Air Force has committed to complete their migration by the end of next year. If confirmed, I will continue to partner closely with the Services as we build out the CES program to ensure that it adequately addresses the entire lifecycle from recruiting, to training, to retaining cyber talent.

92. **In your judgement, what additional authority does the Department needs to help further recruit and retain talent to the Cyber Excepted Service?**

At this time, I do not believe we need any additional authority; we need to focus on building out the program, including defining retention incentives, pay incentives, and training. I will aggressively pursue these initiatives if confirmed.

93. **Should management of the Cyber Excepted Service be transferred to the Under Secretary of Defense for Personnel and Readiness?**

We work closely with USD(P&R) on implementation of Cyber Excepted Service, but we have agreed that DOD CIO is the right functional lead for this issue. Both organizations recognize that success of the program will require close collaboration between our offices.

94. What quantitative and qualitative metrics should be established and tracked to determine the effectiveness of the Cyber Excepted Service, and to support decisions as to whether adjustments to existing authorities are required?

Establishing metrics is a priority for me. I am already tracking CES progress on my scorecard for Cyber Top 10 priorities, including the number of open positions, the time to fill them, and the number of CES migrations. I have given guidance to my team to re-evaluate the metrics that we currently capture to ensure that they will help us to see the leading indicators to ensure we are successful in this space.

<u>Equal Employment Opportunity and Harassment</u>

95. In responding to an inaugural DOD Civilian Employee Workplace and Gender Relations survey administered in 2016, 14.2 percent of women DOD employees and 5.1 percent of men indicated that they had experienced sexual harassment and/or gender discrimination by "someone at work" in the 12 months prior to completing the survey. What is your view of the role of the chain of command/chain of supervision in maintaining a command/workplace climate in which harassment and discrimination are not tolerated?

The Department of Defense relies on its leaders to make some of the most critical decisions an individual can make, and expects the women and men under them to abide. The cornerstone to this is good order and discipline. DOD leadership and senior management must be role models and set the tone – in both words and actions - for all aspects of good order and discipline. This includes ensuring that harassment and discrimination are not tolerated in the workplace.

96. In your view, does the Department's method for tracking the submission and monitoring the resolution of informal complaints of harassment or discrimination provide DOD leaders, supervisors, and managers, with an accurate picture of the systemic prevalence of these adverse behaviors in the civilian workforce?

DOD Instruction 1020.03 "Harassment Prevention and Response in the Armed Forces" was issued in 2018 and establishes a comprehensive, DOD wide military harassment prevention and response program. Accountability and assessments are critical elements of all prevention policies to ensure we understand the scope of these issues in our ranks. As such, this new policy included mechanisms for reporting and tracking reports of harassment. While we are still in the beginning stages of perfecting this accounting system, we are already seeing significant increases in the number of informal complaints we are able to track. Informal complaints include an allegation, made either orally or in writing, to a person in a position of authority within the Service member's organization or outside of the Service member's organization. We hope to continue to make gains in this area using more modernized data analysis approaches and we will continue to report these out annually.

97. Does the Department's method for responding to complaints of harassment or

discrimination in the civilian workforce provide appropriate care and services for victims? For holding offenders appropriately accountable?

The Department has policies in place to address harassment and discrimination in the civilian workforce. While the Department of Defense issued DODI 1020.03 in 2018, due to unique differences in the EEO process for civilians and disparate policies across components, this issuance did not include civilians. To address these unique considerations, the Department established the Defense Equal Opportunity Reform Group (DEORG) in 2018 to develop – collaboratively with the Services – an overarching civilian policy. It is my understanding that this policy is currently in coordination within the Department and we hope to release it this year.

98. In your view, do military and civilian leaders in the DOD have the training, authorities, and resources needed to hold subordinate commanders and supervisors accountable for the prevention of and response to harassment and discrimination? If not, what additional training, authorities, or resources to you believe are needed, and why?

Yes, I believe military and civilian leaders have the necessary training, authorities, and resources to hold subordinate commanders and supervisors accountable, and our surveys indicate the majority of our members trust their leadership in this area. That being said, the Department is always looking for ways to strengthen this authority and works to modify policies accordingly.

99. If confirmed, what specific role and tasks would you establish for yourself in the Office of the DOD CIO program of preventing and responding to harassment and discrimination in the workforce?

Department has a number of efforts in this area under the Office of the Under Secretary of Defense for Personnel and Readiness. If confirmed, I will work closely with that office to ensure that all policies are disseminated widely and they are understood and implemented at all levels within DOD CIO. I will also ensure fair, impartial, and timely investigation and resolution of complaints of harassment and discrimination.

100. In the context of your service to date as the DOD CIO, have you administered a command climate survey to the workforce under your leadership and management? If so, what were the results of that survey and what actions did you take or direct to address the survey results? If you have not administered such a survey, do you have plans to do so, if confirmed?

In addition to encouraging my organization's participation in the Federal Employee Viewpoint Survey, I administered a climate survey in late 2018. Almost 60% of the staff participated and some of the key findings were that employees:

- Were concerned about a lack of stable leadership,
- Felt under-resourced with government personnel,
- Desired more communication up and down and across the organization, and
- Wanted a clear CIO vision and mission with roles/responsibilities defined for all offices.

As a result of the survey I initiated several actions, including putting in a place a leadership team focused on our shared values; drafted a more granular climate survey to get to the heart of what we need to work on; increased communication top down and laterally across the organization; conducted brown bag sessions to get insight directly from our team; undertook an exhaustive analysis of our activities to re-prioritize alignment to our strategy; and reorganized to posture ourselves for success moving forward. We recently received the 2019 Federal Employee Viewpoint Survey results and saw improvements in all areas, which indicates these efforts are having a positive impact.

100. **Given that competent and caring leadership is one of the most significant and relevant levers available to shape a high-performing DOD civilian workforce, if confirmed, what factors and characteristics would be most important to you in selecting a candidate for appointment to the Senior Executive Service (SES) in the DOD CIO enterprise for which you would be responsible?**

I look for leaders that possess astute executive skills. These skills include emotional intelligence, technical competence, fostering teamwork, accountability for delivery, and strategic thinking. If confirmed, these will continue to be the skills that will define my leadership team.

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

The SES under my authority each have as part of their performance plans critical elements associated with "leading people," which assesses whether the executive fosters high ethical standards, provides an inclusive workplace that fosters the development of others to their full potential, while holding employees accountable for appropriate levels of performance and conduct. The SES are also evaluated on recruiting, retaining, and developing the talent needed to achieve a high quality, diverse workforce that reflects the nation, with the skills needed to accomplish organizational performance objectives while supporting workforce diversity, workplace inclusion, and equal employment policies and programs.

102. **Under current law, the civilian pay raise to adjust for wage inflation is set at the Employment Cost Index (ECI) minus 0.5 percent, or about a 2.6 percent increase for FY 2020. Yet, the Department's budget did not provide funding for a civilian pay increase, notwithstanding submission of the largest topline defense budget request in the Nation's history. If confirmed, would you personally support a pay raise for DOD civilian employees, consistent with current law?**

Civilian employees are a key component in supporting the warfighters and the Department's mission to protect our country, so it is important to ensure their pay is not disadvantaged. I would support a pay raise for DOD civilian employees if such a law is enacted.

103. **How would you assess the morale of the DOD CIO civilian workforce? What is your assessment of the effect that past pay and hiring freezes have had on the DOD civilian workforce?**

I believe morale is high among the DOD CIO civilian workforce. We recently received the 2019 Federal Employee Viewpoint Survey results and saw improvements in all areas. Regarding pay, factors like Continuing Resolutions and government shut downs have a de-stabilizing effect, and can result in further negative consequences. At a time when DOD CIO competes heavily with the private sector for technology talent we must ensure competitive compensation for our employees.

Cyber Mission Force

In May 2018, the Cyber Mission Force achieved full operational capability. 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" to compete, deter, and win in the cyber domain.

104. What do you envision as the role of DOD and the Cyber Mission Force in defending the Nation from an attack in cyberspace? In what ways is this role distinct from those of the homeland security and law enforcement communities?

As noted in the DOD Cyber Strategy, DOD's primary focus is on defending forward: seeking to deter, disrupt, or defeat cyber threats near the source, before they harm our networks. When directed by the President or requested by the Department of Homeland Security (DHS), DOD is prepared to assist DHS in the event of a significant cyber incident. DHS and the law enforcement community operate under authorities that are domestically aligned, whereas DOD's focus is addressing threats overseas.

105. How will operationalization of the "defend forward, shape the day-to-day competition, and prepare for war" concepts deter and disrupt Russia and China's aggression in cyberspace?

China and Russia are conducting persistent malicious cyber campaigns to erode U.S. military advantages, threaten our infrastructure, and reduce our economic prosperity. DOD is taking the initiative to deny, disrupt, degrade, and expose these malicious cyber activities, which threaten the Department, U.S. interests, and the American people. We seek to proactively address and disrupt these threats well before these activities reach their intended targets and cause harm. Operationalizing these concepts enables us to shape behavior by raising adversary costs for malicious cyber activity and denying their intended benefit.

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

Routinely operating below the level of armed conflict is both feasible and necessary in cyberspace, as in all other domains. We need to engage our adversaries and defend forward persistently to disrupt, deter, and defeat malicious cyber activity. These operations range from intelligence collection and preparation to strengthening the security and resilience of our cyber networks. DOD can focus these efforts on states that conduct malicious cyber activities and that pose strategic threats to U.S. security and prosperity, while collaborating with our interagency, industry, and international partners.

107. What role should DOD and the Cyber Mission Force occupy in combating foreign

influence operations, especially those conducted via social media?

The DOD Cyber Strategy's concept of defending forward includes monitoring malicious cyber actors' behavior, warning of imminent threats, and remaining postured to take action against those threats. The Cyber National Mission Force plays a significant role in these efforts. The DOD also contributes to a whole-of-government to support two-way sharing of cyber threat information with the private sector and to collaborate on efforts to prevent cyber-enabled influence operations.

108. What role should DOD and the Cyber Mission Force occupy in anticipating, preventing, or responding to attacks on commercial entities?

DOD is executing a series of "Pathfinder" initiatives on critical infrastructure protection in partnership with DHS and sector-specific agencies for finance and energy. These initiatives are helping our organizations build the collaborative expertise and experience needed to anticipate, prevent, and respond to significant cyber incidents. Specifically, we have focused on lessons learned from our election security efforts, and have focused on sharing threat information and collaborative analysis of vulnerabilities and threats. The Department also plans to utilize the National Guard's unique resources and capabilities for this mission, and to expand these partnerships to other critical sectors where DOD and the private sector have shared interests.

109. What is your view 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? Please explain your answer.

The central challenge is balancing the USCYBERCOM and NSA responsibilities and priorities in a way that is optimal for national security. Any DOD recommendation to the President will require careful collaboration and coordination with the Chairman of the Joint Chiefs of Staff and the Director of National Intelligence, and must be fully informed by the benefits, costs, and risk mitigation factors. Regardless of whether the leadership of these two organizations remains dual-hatted, the organizations will continue to have a unique and enduring relationship.

In March 2019, the Secretary of the Navy's *Cyber Readiness Review* presented a scathing assessment of the Department of the Navy's approach to cybersecurity and hi-lighted the urgent need for the Navy to modify its business and data hygiene processes to protect data as a resource.

110. In your view, would DOD writ large benefit from a "Cyber Readiness Review" similar to that of the Navy? Please explain your answer.

I strongly believe that we need to treat DOD networks and computing infrastructure as any other weapon system and consider its configuration a readiness issue. The DOD Cyber Hygiene Scorecard helps convey the importance of this issue, capturing 12 key measures of the readiness posture of DOD IT infrastructure. It functions as a "Cyber Readiness Review" for the DOD as a whole and, with the DOD Cyber Top 10 priorities, allows DOD senior leadership to quantitatively track cybersecurity progress and risk reduction.

111. If confirmed, specifically what measures would you take or direct to improve the cybersecurity culture across the DOD workforce—military, civilian, and contractor? How would you empower and hold key leaders accountable for improvements in DOD cybersecurity?

If confirmed, I will continue to ensure senior leaders are informed and engaged in addressing the DOD Top 10 Cyber priorities. This includes continuing to provide clear, quantitative metrics and scorecards to promote transparency about DOD cyber risks and accountability for mitigations. If specific systems and networks are holding the larger DOD at risk, I, in coordination with USCYBERCOM, have been directing that noncompliant enclaves be isolated from the larger environment. I co-chair a forum where senior leaders responsible for improving cybersecurity are expected to update the Deputy Secretary of Defense on their remediation progress and any implementation challenges.

Insider Threat

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 National Insider Threat Task Force published the Insider Threat Program Maturity Framework in November 2018.

112. 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 reach a critical point and potentially harm national security.

The realignment of the Defense Security Service to become the Defense Counterintelligence and Security Agency is a significant step towards improvements in personnel vetting and counterintelligence. I believe DCSA will strengthen and improve the Department's posture for deterring, detecting, and mitigating insider threats, as well as external threats posed by foreign intelligence and other threats to our people, programs, and information. This includes plans for expanding the Department's use of User Activity Monitoring, Continuous Evaluation, and Insider Threat hubs as our primary "sensors" for staying ahead of potential problems that lead to attacks by malicious insiders.

113. If confirmed, specifically what would you do to ensure that senior leaders across the DOD CIO enterprise—are fully invested in protecting their people, facilities, and information from insider threats as a core mission objective?

Addressing insider threats is one of the DOD Top 10 Cyber priorities and a major line of effort for DOD Cyber Strategy implementation. The combined efforts of the DOD CIO, USD(I), and

PCA have led to increased funding for the development of Insider Threat hubs in 41 DOD components. These funds have enabled the Department to deploy User Activity Monitoring tools on our classified networks, and to develop the analytic capability to use User Activity Monitoring data to detect and mitigate insider threats. As noted earlier, the realignment of the Defense Security Service to become the Defense Counterintelligence and Security Agency is also strengthening the Department's posture for deterring, detecting, and mitigating insider threats. If confirmed, I will sustain this partnership with USD(I) and the PCA, pursuing additional digital modernization initiatives addressing insider threats and personnel vetting.

<u>Security Clearance Reform</u>

By Executive Order dated April 24, 2019, President Trump directed transfer to DOD of the background investigation mission presently executed by the Office of Personnel Management through its National Background Investigations Bureau. DCSA will be the primary entity for the conduct of background investigations to inform security clearance, employment suitability, and credentialing determinations for the entirety of the Federal Government. As well, DCSA will serve as the DOD proponent for the National Industrial Security Program; operate the continuous vetting and insider threat programs; and undertake other responsibilities as assigned by the Secretary of Defense.

114. The Defense Information Systems Agency has been vested with responsibility for modernizing the National Background Investigation System (NBIS). What is your vision for success in this critical project? What progress has been made to date? On what timeline can we expect modernization of NBIS to evolve and when will modernization be complete. At what point can DOD expect measureable improvements in the timeliness and completeness of DOD background investigations? What metrics have you established to measure and assess progress toward these goals?

The Deputy Secretary of Defense directed that the NBIS program transition from DISA to the Director of Defense Counterintelligence and Security Agency earlier this year.

<u>Relations with Congress</u>

115. What are your views on the state of the relationship between the Office of the Chief Information Officer and the Senate Armed Services Committee in particular and with Congress in general?

I believe that the state of the relationship between the Office of the Chief Information Officer and the Senate Armed Services Committee, in particular, and with Congress, in general, is strong. From the very beginning of my tenure, I have made timely and accurate communications with Members of Congress and congressional staff one of my top priorities. I cannot succeed in delivering digital modernization without strong partnership with Congress.

116. If confirmed, what actions would you take to sustain a productive and mutually beneficial relationship between Congress and the Office of the Chief Information

Officer?

If confirmed, I will maintain transparency with both Members and Congressional Staff, via the Assistant Secretary of Defense for Legislative Affairs, and provide timely, accurate, and thorough responses to all requests for information from Congress. I strongly support having staffer and Member visits and maintaining open lines of communication.

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.

117. Do you agree, if confirmed, and on request, to appear and testify before this Committee, its subcommittees, and other appropriate committees of Congress?

Yes.

118. Do you agree, 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?

If confirmed, I agree to accommodate in a timely manner all congressional requests for information by supplying the requested information to the fullest extent, consistent with applicable statutes and the U.S. Constitution.

119. Do you agree, 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?

Yes.

120. Do you agree, 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?

Yes.

121. Do you agree, 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?

If confirmed, I agree to accommodate all congressional requests for information by supplying the requested information to the fullest extent, consistent with applicable statutes and the U.S. Constitution.

122. Do you agree, 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?

If confirmed, I agree to accommodate all congressional requests for information by supplying the requested information to the fullest extent, consistent with applicable statutes and the U.S. Constitution.

123. Do you agree, 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?

Yes, I agree to protect DoD personnel from unlawful retaliation.