Senate Armed Services Committee
Advance Policy Questions for Mr. John Sherman
Nominee for Appointment to be Department of Defense Chief Information Officer

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.

What is your understanding of the duties and functions of the CIO?

It is my understanding that the DoD CIO serves as the primary advisor to the Secretary of Defense for information technology, management, and assurance; as well as non-intelligence space systems, critical satellite communications, navigation and timing programs; spectrum, and telecommunications. Additionally, I understand that the DoD CIO drives technology and cyber transformation to ensure warfighters maintain a decisive advantage over adversaries, works with industry to identify new solutions, advocates for IT and cyber talent, and leads CIOs and other stakeholders from across the Department towards modernization goals.

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

If confirmed, I expect that oversight of the Cyber Maturity Model Certification (CMMC) activities might be transferred from USD(A&S) to the DoD CIO portfolio, under the DoD Chief Information Security Officer (CISO). In this scenario, DoD CIO/CISO would provide the centralized cybersecurity oversight of the CMMC activities, with USD(A&S) maintaining the Department's lead role for overall engagement with the Defense Industrial Base.

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 Principal Deputy DOD Chief Information Officer, that you would apply to your service as CIO, if confirmed.

My foundation for the DoD CIO role includes serving as the Intelligence Community (IC) CIO, the DoD Principal Deputy CIO (PDCIO), and the Acting DoD CIO. All involved experiences with strategic leadership of large-scale technology modernizations, which I would apply to the DoD CIO role if confirmed. As the IC CIO, I oversaw the flagship IC Information Technology Enterprise initiative, where I led major updates to cloud computing, cybersecurity, and interoperability during my nearly three years in the job. At DoD, I oversaw the shift to the enduring DoD365 collaboration and productivity suite, accelerated the focus on Zero Trust for cybersecurity, moved to meet urgent cloud-computing needs with the Joint Warfighting Cloud Capability (JWCC) multi-cloud

approach, increased emphasis on resilient Positioning, Navigation, and Timing (PNT), and launched a new strategy to diversify and strengthen our cyber talent. All of this is undergirded by my nearly 25 years in the IC as a consumer and user of cutting-edge technology.

Given your observations and experience to date as the Principal Deputy 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?

If confirmed, one of my main priorities would be to implement Zero Trust across the Department, changing the cybersecurity paradigm from one of protecting perimeters to one that assumes adversary penetration of the network and employs principles of micro-segmentation. Additionally, I would focus on deployment of an enterprise multi-cloud solution with JWCC, which is critical to enable Joint All-Domain Command and Control (JADC2). I would also work with Department stakeholders to identify and deploy increasingly innovative and complementary types of PNT to ensure resiliency against growing threats. Finally, I would work with DoD components, Executive Branch departments, Congress, and industry on ways to ensure warfighter access to critical electromagnetic spectrum capabilities while also identifying opportunities to help strengthen US 5G advantage.

Major Challenges and Opportunities

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

Ensuring cybersecurity of the Department of Defense Information Network (DoDIN) in the face of increasingly capable threats would be among my top challenges if confirmed. Additionally, providing edge-node capabilities in support of JADC2, such as in the Western Pacific and in a highly-contested battlespace, would also represent a major task to be addressed. Finally, DoD's ability to recruit, retain, and reskill IT and cyber talent, especially in an environment of increasing competition for key skillsets, represents both a challenge and an opportunity to reimagine how DoD manages its civilian and uniformed technology professionals.

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

I began strengthening the Department's cybersecurity posture as Acting CIO by moving the enterprise towards a Zero Trust footing, overseeing the Defense Information Systems Agency's (DISA's) launch of the "Thunder Dome" Zero Trust initiative, the publication of a Zero Trust reference architecture, and the preparations for the standup of a Zero Trust portfolio management office within DoD CIO. If confirmed, I would move out quickly on implementing the key elements of Zero Trust, starting with deployment of enterprise Identity, Credential, and Access Management (ICAM) in early 2022. Also, I

would immediately build upon the partnership between CIO organization and the Director, Operational Test and Evaluation (DOT&E), which was instrumental in the testing of DoD365 earlier this year and will be vital as we ensure the cyber bona fides of commercial cloud capabilities. On support to JADC2, in July 2021 I launched the pivot to the JWCC multi-cloud approach, which will provide enterprise cloud computing capabilities, at all three security levels, from the Continental United States to tactical edge environments. While fully recused from developments on this procurement since my nomination in September 2021, I established the 3Q FY22 award date while still serving as the Acting CIO. Finally, I launched the drafting of a cyber-talent strategy earlier this year, with a projected publication date of early-to-mid 2022.

Describe significant opportunities in the domain of the DOD CIO that, in your view, and informed by your service as Principal Deputy CIO, DOD has not fully leveraged.

Based on my time here in the Department since June 2020, I believe that DoD is fully leveraging all facets of the DoD Digital Modernization Strategy (DMS) with regards to cloud, cybersecurity, data, AI, and command, control, and communications. Deployment of modernized capabilities and enhancements, ranging from strengthened weapons system cybersecurity to deployments of resilient PNT across the force to implementation of the Electromagnetic Superiority Spectrum Strategy (EMS3), at the speed and scale necessary to stay ahead of the China pacing threat, remains an opportunity for continued progress in the CIO domain.

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

If confirmed, I would leverage established governance venues at the enterprise and CIO levels to drive component action on areas needing acceleration (remediation of cybersecurity threats, etc.) and provide strong, active oversight of Military Department investments through planning guidance and budget certification processes. I would also work through less formal channels, such as by day-to-day engagements with CIOs and other leaders, to sustain unrelenting focus on developing and deploying critical capabilities, at speed and scale.

If confirmed, what follow-on actions (e.g., sustainment, enhancement, modification, termination) would you take with regard to initiatives established by your predecessor, specifically digital modernization, composed of cybersecurity, data management, enterprise cloud, artificial intelligence, and joint all-domain command and control? Please explain your answers.

If confirmed, I would continue efforts against all facets of the DoD DMS launched by my predecessor, with appropriate updates in areas such as Zero Trust for cybersecurity, an enterprise multi-cloud approach, oversight of EMS3 implementation, and other developments and opportunities that arise in the constantly-evolving technology and cybersecurity space. A "North Star" for modernization efforts would be towards enabling

joint warfighting and JADC2, especially in support of combat operations in highly-contested, edge environments.

Your predecessor concluded that these initiatives required additional personnel with engineering and other technical expertise, but was unable to gain approval for these additional billets.

Based on your experience to date as the Principal Deputy and Acting CIO, what is your view as to whether the CIO's office requires additional manpower and expertise to properly implement these initiatives?

Based on my experience in DoD CIO, both as Principal Deputy and Acting CIO, I believe that the CIO's office is properly staffed for its mission. I would reassess this if confirmed, and on an ongoing basis, especially in light of additional responsibilities for CIO in areas such as Zero Trust, EMS3, and 5G.

Historically, the DOD CIO, as well as the CIOs of the military departments, have been perceived as lacking operational expertise and have been more or less confined to non-warfighting and non-operational roles. Today, however, the lines between protecting and managing administrative information technology networks and operational warfighting networks have blurred and integrated enterprise networks face common cyber and information warfare threats. CIO's are also increasingly called upon to manage information technology initiatives that directly impact operational capabilities.

Should DOD CIOs be, and be seen as, more involved in military operational matters, in your view?

Yes, at the strategic level. The Department's ability to counter advanced adversaries like China and Russia is heavily reliant on the digital modernization capabilities that the CIO oversees.

In your view, should CIOs across the DOD Components acquire more operational expertise to be effective in their jobs?

Based on my experience, the CIOs in the components are highly knowledgeable of their respective organization's operational needs, and they adapt and deploy technology accordingly.

If so, how would such capabilities be acquired and documented?

A Component CIO's ability to understand and address operational needs should be documented in artifacts such as position descriptions and vacancies. Also, familiarity with military operations and technology requirements to support current doctrine and strategies should be a key consideration in hiring.

The DOD CIO is responsible for a plethora topics that affect DOD business and military operations. Is the office organizationally aligned correctly? Does it have sufficient staff to meet its responsibilities and obligations?

Based on my experience, the DoD CIO organization is properly aligned and has sufficient staff to meet its responsibilities and obligations. As Acting CIO, I elevated the Special Access Program (SAP) IT portfolio to a Deputy CIO level in order to ensure the topic received appropriate effort and leadership attention. If confirmed, I would continually assess all areas of CIO, similar to what I did for the SAP IT function, and make necessary adjustments and/or advocate for additional resources.

Civilian Control of the Military

If confirmed, specifically what would you do to ensure that your tenure as CIO 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 fundamental principle of the Constitution, which I would firmly uphold and protect if confirmed. If confirmed, I would provide proper and adequate direction and meaningful civilian oversight in the course of my duties, and advocate to ensure that the office of the DoD CIO has appropriate staffing to perform the required civilian oversight.

2018 National Defense Strategy

The 2018 National Defense Strategy (NDS) outlined three lines of effort by which the U.S. would generate decisive and sustained military advantage in great power competition and conflict: 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.

Do you believe DOD has been successful in implementing the 2018 NDS? Why or why not? In which lines of effort and nested tasks do you perceive a need for continued improvement or additional focus or resources? Please explain your answers.

I believe DoD has been successful in large part with implementing major aspects of the 2018 NDS, especially with regards to refocusing efforts from counterinsurgency to greater lethality against nation-state adversaries. Additionally, a continued focus on strengthening key partnerships across many regions and nations has bolstered DoD, and reforms have resulted in new achievements like the Fourth Estate Network Optimization (4ENO) initiative. In terms of additional focus going forward, especially in a CIO context, a continued and robust effort to ensure US weapon systems and networks are hardened against near-peer adversary threats must be a priority, along with development

of new capabilities in areas such artificial intelligence (AI), compute and transport in edge/contested environments, agile software development (DevSecOps), the future shift to 6G, even more resilient PNT, and enabling full dominance of the electromagnetic spectrum (EMS).

Relationships with Other Department Offices

What is your understanding of the respective responsibilities of the Principal Cyber Advisor and the CIO regarding the Department's cyber activities and cybersecurity programs and architecture?

The DoD CIO is responsible for establishing policies, standards, and architectures to ensure networks and systems are capable of operating in any environment. The DoD CIO also provides budgetary and programmatic oversight of Military Departments, Defense Agencies and Field Activities (DAFAs), to include the National Security Agency's (NSA's) Cybersecurity Directorate. In addition to its oversight of U.S. Cyber Command (USCYBERCOM), the Principal Cyber Advisor (PCA) monitors the execution of the DoD Cyber Strategy and integrates cyber operations policy, programs, and processes across the Department, to include cybersecurity objectives under DoD CIO responsibility.

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

If confirmed, I would work with USD(P) and other stakeholders to review the allocation of responsibilities to ensure the Department's cyber mission is being carried out efficiently and effectively, and then make recommendations as needed to Department leadership.

What is your understanding of the respective responsibilities of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) and the CIO for the acquisition of cybersecurity, information technology, and command, control, and communications systems, including contracting and software development? For securing the Defense Industrial Base against cyber attacks? For supervising the Strategic Cybersecurity Program?

USD(A&S) has oversight of the acquisition process and promulgation of acquisition policy to ensure that acquisition programs implement DoD cyber security policy throughout the entire acquisition lifecycle. The DoD CIO works with USD(A&S) to ensure that system acquisitions are compliant with DoD cybersecurity architectures, policies, and standards. These responsibilities also apply to the Strategic Cybersecurity Program (SCP) where DoD CIO works in conjunction with USD(A&S) and other SCP stakeholders to assure the cybersecurity of weapon systems and critical infrastructure across the acquisition lifecycle.

Do any of these allocations of responsibilities need to be changed or clarified, in your view? Please explain your answer.

At this time, I do not believe the overall allocations of responsibilities need to be changed or clarified. As the Department's senior acquisition official, USD(A&S) is able to leverage its authorities and oversight to ensure the incorporation of cybersecurity, and adherence to DoD CIO promulgated cybersecurity policies, architectures, and standards, in the acquisition of goods and services. Also, I believe there might be a transfer of responsibilities for the cybersecurity oversight of the CMMC program from USD(A&S) to CIO, with USD(A&S) maintaining overall lead for DIB engagement and related issues. If confirmed, I will continue to work with USD(A&S) to align acquisition and cybersecurity policy while identifying any gaps that may arise in our joint cyber assurance responsibilities.

What is your understanding of the respective general 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 and other emerging technologies?

The USD(R&E) is responsible for fundamental AI research and developmental prototyping of AI capabilities, and collaborates closely with DoD Components to improve the capacity to transition such capabilities to production, integration, and operational use. In short, USD(R&E) is responsible for advancing the state of the art in AI.

The USD(A&S) plays a critical role in updating policies on software acquisition, including systems that are enabled by AI software. USD(A&S) is also responsible for training the DoD acquisition workforce, and the JAIC has been a close partner in training this community on best practices in AI acquisition.

The Military Departments continue their mission of "man, train, and equip," and the JAIC seeks to provide enabling services to, for example, program offices to accelerate their incorporation of AI capability.

In a 2019 memorandum, the then-Deputy Secretary of Defense designated the Director of the JAIC as the senior designated official for AI, as required by Sec. 238 of the FY 2019 NDAA. The Senior Official role includes principal responsibility for the coordination of activities relating to the development and demonstration of AI and machine learning for the Department. As the JAIC is now a direct report to the Deputy Secretary of Defense, the JAIC Director meets regularly with the DoD CIO to ensure synchronization across the information enterprise, especially on enterprise priorities such as the AI and Data Accelerator (ADA) Initiative.

More specifically, what is your understanding of the CIO's continued responsibilities for artificial intelligence once the Director of the Joint Artificial Intelligence Center is realigned to report directly to the Deputy Secretary of Defense?

The DoD CIO will continue to play an important enabling function in DoD AI transformation through its management of the foundational networks, platforms, IT infrastructure, and policies that facilitate AI capability development. The DoD CIO and the JAIC are close partners in executing the ADA Initiative, and the DoD CIO serves as a member of the ADA Implementation Management Executive Steering Group, which oversees the ADA Initiative.

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

In my view, this allocation of responsibilities is appropriate to ensure the necessary implementation and integration of AI within the Department, while also ensuring the DoD CIO and JAIC continue to collaborate seamlessly on key issues and projects.

What is your understanding of the respective roles and responsibilities of the CIO and the DOD Chief Data Officer, who will now report directly to the Deputy Secretary of Defense, with respect to data policy, standards, and architectures?

Currently, the DoD Chief Data Officer (CDO) reports to the DoD CIO. Both DoD CIO and CDO have complementary roles with respect to policy, standards, and architectures. The DoD CDO governs the development of data-related policies, standards, and architectures which ensure data is visible and accessible in an open, non-proprietary format. The DoD CIO leads the development and implementation of the IT and transport architecture that move data to the point of need, as well as the cybersecurity that protects the data. My experience in the IC has shown the benefit of having these as distinct roles working in peer-level partnership.

What is your understanding of the respective responsibilities of the USD(R&E), USD(A&S), and the CIO in prioritizing research and development activities that will provide enhanced information enterprise capabilities for the future of the DOD?

My understanding is that emerging technology is typically first identified by USD(R&E) professionals. As the technology begins to mature, either organically or in the commercial space, DoD CIO partners with USD(R&E) to ensure relevant IT capabilities, policy, and guidance are in place. Collectively, our collaboration ensures USD(A&S) has both the relevant acquisition pathway identified and baseline level of technological understanding to complete a system's journey from research to pilot to operational deployment. I believe that all three organizations—CIO, USD(R&E), and USD(A&S)—are critical to achieving digital modernization and, if confirmed, I am committed to working with both organizations to provide enhanced information enterprise capabilities to the DoD.

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 National Defense Authorization Act (NDAA) for Fiscal Year

(FY) 2019, the CIO, and the Principal Information Operations Advisor to the Secretary of Defense, for the management of electronic warfare; electromagnetic operations, standards, and policy; and information operations?

The Executive Committee on Electronic Warfare (EWEXCOM) functions as an advisory body to key senior level DoD decision bodies on investment, development, acquisition, sustainment, and intelligence integration on Electronic Warfare (EW) investments.

The Senior Designated Official (SDO) of the EMSO Cross-Functional Team (CFT) has two primary areas of responsibility: (1) provide recommendations on resource allocation and investments in the EMSO mission areas; and (2) propose EMSO governance, and operational reforms to the Secretary of Defense through the EWEXCOM. The SDO is in the process of transferring EMS3 execution and oversight responsibilities to the CIO.

Pursuant to Department of Defense Directive 3610.01, the DoD CIO, as the Principal Staff Assistant (PSA) for EMS: (1) advises the Secretary of Defense on matters related to the EMS and EMS regulatory activities globally, including national and international fora; (2) develops and provides guidance on DoD strategies and policies in support of operations in the EMS; (3) informs DoD strategies on EMS command, control, and coordination system investments; (4) develops instructions to clarify EMS roles and responsibilities in greater detail; (5) advises the DoD Component heads on DoD investment strategies for EMS-dependent systems; (6) establishes a review and evaluation process that considers all EMS requirements; (7) ensures all DoD EMS users are involved in all DoD spectrum-related decision-making processes; and (8) in coordination with the USD(R&E), USD(A&S), and the Chairman of the Joint Chiefs of Staff, provides oversight of EMS-related capability development to the EWEXCOM as the governance structure.

Pursuant to 10 US Code 397, the USD(P) serves as the Principal Information Operations Advisor to the Secretary of Defense, and provides advice on all aspects of information operations conducted by the Department, including support operations, electromagnetic warfare, special technical operations, operations security, cyberspace operations, and military deception.

Do these allocations of responsibilities need to be changed or clarified, in your view? Please explain your answer.

It is my understanding that revisions to DoD Directive 5144.02 are in progress and that these will clarify the CIO's EMS governance responsibilities. Multiple studies have revealed governance as a major challenge for DoD spectrum operations, including dispersed responsibilities across the Department at various organizational levels. The entire Department is embracing an enterprise approach to create unity of effort across the organizations and is aligning EMS efforts.

What do you perceive to be the appropriate relationship between the DOD CIO, the CIOs of the Military Departments and Defense Agencies, and the Joint Staff J6?

I believe the DoD CIO must set the strategy and direction for digital modernization priorities and lead the DoD technology enterprise. There should be close collaboration with the other CIOs and the Joint Staff (JS) J6, with the DoD CIO facilitating partnership, sharing of best practices, a willingness to hear suggestions, and an environment to make changes when better solutions or approaches arise. The DoD CIO must also be attuned to the operational needs conveyed by the other CIOs and JS J6, and ensure that Department initiatives don't occur at the expense of user experience and mission effectiveness. All the while, the DoD CIO must ensure adherence to standards, strategic guidance, and policies—holding a hard line where necessary, while also maintaining flexibility to capitalize on emerging opportunities. Success relies on close communication, trust, and transparency between the DoD CIO and the other IT and cyber leaders.

If confirmed, how would you ensure consistency of approach and unity of effort to strategy development, planning, policy making, and oversight, in the information enterprise across the Department of Defense?

If confirmed, I would partner and meet frequently with the CIOs of the Military Departments, including the US Coast Guard, National Guard Bureau, Commander USCYBERCOM, and Director of DISA, to establish the right strategy to collaboratively develop and maintain a modern and dynamic information enterprise that is cyber-secure and responsive to the Department's needs. I would also consider establishing and/or strengthening joint governance forums to vet issues and ensure consistent implementation of infrastructure enhancements, with a special focus on leveraging commercial solutions to get the best capabilities to our users in the shortest period of time while enhancing security and minimizing cost.

If confirmed, how would you avoid unnecessary duplication between your efforts as the Department's CIO and the CIOs for each of the Military Departments?

If confirmed, I would avoid duplication of efforts with the Military Departments through governance, communications, and oversight empowered by data-driven analytics via the Advana platform. If we identified a redundant or duplicative activity, I would direct that we quickly review its rationale and determine whether it should proceed, and, if not, how the requirement could be met using a current or forthcoming enterprise capability.

In your role as the Principal Deputy CIO, 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 or will rectify the situation. If confirmed, what systemic changes would you introduce to avoid this same circumstance going forward?

Defending our nation and ideals of freedom is no longer confined to traditional battlefields, with adversaries now targeting not just our military facilities, defensive assets, and soldiers, but also the networks, critical infrastructure, and individual citizens that support our way of life. Their weapon and target of choice is information and data**.**

Improving the Department's technological agility and speed while enhancing our cyber posture remains a critical challenge, one that requires a comprehensive approach driven as a collaborative effort by the Department's leadership. If confirmed, I would continue to work along with the USD(A&S), USD(R&E), and other stakeholders to push rapid technical improvement, agility, and resiliency through the Department's Software Modernization initiative and other priorities in the DoD DMS.

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, and in assessing and correcting information technology-related problems across the Department?

It is my understanding that DoD CIO and the Defense Digital Service (DDS) are well-aligned. There is a shared desire to improve the way software is designed, developed, deployed, and secured across the Department. DDS is a proven source of innovation inside the Department and provides perspectives that have led to cultural changes with how DoD approaches software development. The Department is working to adopt, adapt, and scale both their methodology and its tools. In addition, DDS has been a strong partner to CIO in designing and implementing next-generation network security solutions, such as Zero Trust and cloud computing.

What do you perceive to be the appropriate relationship between the DOD CIO and the Principal Cyber Advisor to the Secretary of Defense?

The PCA provides the DoD CIO insight into cyber policy and broader perspectives on areas dealing with oversight of USCYBERCOM, while the CIO provides the PCA with an understanding of enterprise-level IT modernization and defensive cyber activities. There should always be a close partnership between the PCA and CIO, especially on areas such as the SCP, the nexus between offensive cyber strategy and the CIO's defense cybersecurity portfolio, cyber investment strategy, and advocacy for cyber talent and education within the Department.

How do you assess the current division of labor in cybersecurity between the DOD CIO, the USD(A&S), the Under Secretary of Defense for Intelligence and Security (USD(I&S)), and the Under Secretary of Defense for Policy (USD(P)) in securing the Defense Industrial Base and Defense Critical Infrastructure?

Securing the DIB and Defense Critical Infrastructure against a determined and well-resourced adversary requires a coordinated team effort. DoD CIO, USD(A&S), USD(I&S), and USD(P) work in coordination with one another to accomplish this objective. The Department must understand the intent and ability of our adversaries through intelligence programs administered by USD(I&S), develop and oversee execution of cybersecurity policies, standards, and architectures through the efforts of DoD CIO, ensure that programs and acquisitions adhere to cybersecurity best practices through the oversight of USD(A&S) and ensure effective cross-functional coordination and mission assurance through the efforts of USD(P).

How do you envision the coordination and integration of cybersecurity architectures and capabilities under the oversight of the CIO with those under the direct supervision of Commander, U.S. Cyber Command, such that they complement and support each other, as directed by Congress in law?

The Department maintains the DoD Cybersecurity Reference Architecture (CSRA), which is the foundational guidance for the implementation of cybersecurity capabilities. DoD CIO works closely with USCYBERCOM and the Services to maintain the CSRA and develop capability-specific architectures such as the ICAM Reference Design and the Zero Trust Reference Architecture. If confirmed, as the need for new capabilities or modernization is identified, I would ensure USCYBERCOM and DoD CIO would work together to determine the best approach to address gaps and ensure DoD networks and information are properly protected. USCYBERCOM is a key participant in DoD governance bodies and in developing cybersecurity capability requirements and implementation guidance with DoD CIO.

Please explain how, if confirmed, you would plan to improve coordination with Joint Force Headquarters-DODIN (and CYBERCOM) with its operational responsibilities to protect DOD information networks.

If confirmed, I would look for ways to better leverage JFHQ-DODIN's operational chain of command to publish and enforce cyber tasking orders on high-priority cybersecurity issues. When cyber threats are discovered and a tasking order has been issued, it is critical the threats are remediated quickly.

In your view, where do DOD CIO and Joint Force Headquarters-DODIN (and CYBERCOM) have shared responsibilities and separate responsibilities in protecting the DOD information network?

The DoD CIO is the PSA and senior advisor to the Secretary of Defense for IT, and in that capacity develops DoD strategy and policy on the operation and protection of all DoD IT and information systems, including development and promulgation of enterprise-wide architecture requirements and technical standards, and enforcement, operation, and maintenance of systems, interoperability, collaboration, and interface between DoD and non-DoD systems. Through the DoD CISO, the office of the DoD CIO establishes the DoD Cybersecurity Program, and is the Chief DoD Cybersecurity Risk Manager. The Commander of USCYBERCOM directs the security, operations, and defense of the DoDIN, in accordance with the Unified Command Plan. The Commander of USCYBERCOM has delegated authority to the JFHQ-DODIN to command and control, plan, direct, coordinate, integrate, and synchronize DoDIN operations and defensive cyberspace operations—internal defense measures in order to secure, operate, and defend the DoDIN. Thus, there is a significant shared responsibility in the securing and defending of the networks. The DoD CIO develops the strategy and policy, and strategic risk acceptance tolerance in partnership with USCYBERCOM, which USCYBERCOM and JFHQ-DODIN implement in day-to-day cyber defensive operations.

What do you view as the appropriate role of, and relationship between, the DOD CIO and the Director of the National Security Agency with respect to securing National Security Systems across the government?

The Director of NSA is also the National Security Systems (NSS) National Manager and in that role is responsible to the Secretary of Defense for the security of NSS and to the Director of National Intelligence for those NSS that also qualify as intelligence systems. The DoD CIO ensures compliance with the requirements of National Security Directive (NSD) 42, which is the policy for the security of National Security Telecommunications and Information Systems, and collaborates with the National Manager on the performance of the National Manager's duties, per Executive Order 12333, as to all systems within the DoD. Outside of DoD, the DoD CIO chairs the Committee on National Security Systems (CNSS), which sets policy for NSS across the government.

What do you view as the appropriate role for the DOD CIO Officer vis-à-vis the USD(A&S), the USD(I&S), and the USD(R&E) in securing the Defense Industrial Base and other national security research and technology organizations from adversary cyber threats so as to ensure the integrity and security of DOD's classified information, controlled unclassified information, and other key data?

In my view, the current role is appropriate as the DoD CIO, in coordination with the Defense Cyber Crime Center (DC3) and NSA's Cybersecurity Directorate, maintains an active program of sharing cyber threat information and responds to adversary activity. This partnership extends to USD(A&S), which is responsible for planning, coordinating, and synchronizing cybersecurity throughout the DIB; USD(I&S), which is responsible for developing guidance for and overseeing the DoD industrial security program; and USD(R&E), which is responsible for working closely with the DIB on new technologies, to include in the cybersecurity realm.

Acquisition of Information Technology and Cyber Infrastructure and Capabilities

How can the DOD CIO encourage the appropriate use of rapid acquisition approaches and the "agile" method in regard to software development?

Many software-intensive systems would benefit by transitioning to a software acquisition pathway that demands adoption of modern software development techniques, including agile practices. To drive this change in approach, I understand that DoD CIO partnered with USD(A&S) to release the DoD Enterprise DevSecOps Strategy Guidance. In addition, DoD CIO is driving the adoption of enterprise services that are specifically aligned to software development tooling and expressly linked to acquisition pathways that are agile by design.

What are your views on the role of data and data science in supporting information system acquisitions and the "agile" lifecycle?

I believe that increased use of data is critical to informing and managing all of our acquisition processes, particularly information systems and modern software. As DoD modernizes its approach to make use of "agile" approaches, data engineers and data scientists will increasingly be integral members of the Department's software development teams. They are critical enablers of modernized software Development, Security and Operations (DevSecOps), which will result in increased delivery speed, security, and performance.

In your view, does the existing Department of Defense budgeting, programming, and acquisition process suffice for information technology acquisition, particularly software-intensive work, or do you plan to review such processes?

In my view, existing Department of Defense budgeting, programming, and acquisition processes are aligned to meet the Department's mission. In addition to the Department's overarching Planning, Programming, Budget and Execution (PPBE) and acquisition processes, I understand that the Department recently issued updated software acquisition policy that provides an adaptive acquisition framework to enable delivery of effective, resilient, supportable, and affordable solutions to end users in a timely manner.

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?

I believe that adapting the Department's routine day-to-day business processes in order to realize the cost savings found in adopting commercial information technology systems must become the norm. NSS, however, bring additional complexity, with mission execution parameters being highly rigid for very specific reasons. In this space, successful mission execution justifies the Department's investment for specific mission needs into government-unique solutions. I believe that the balance of commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) products is justified within the Department, but care must be given to ensure balance based on mission need.

How should DOD balance the procurement of information technology- and cybersecurity-as-a-service and the requirement to use the government workforce to perform enduring missions and inherently governmental functions?

I understand that the Department takes a risk-based approach to the procurement of IT and cybersecurity-as-a-service, seeking maximum effectiveness for the warfighter with an eye toward overall affordability and placement of inherently governmental functions. The Department also weighs risk when making decisions regarding its workforce mix, and the DoD CIO has implemented an adaptable the DoD Cyber Workforce Framework (DCWF) to enhance the development and preparedness of its total force as the scope continues to evolve.

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

DISA provides a unique and enterprise-wide mission set of applications and services used by every Combatant Command (CCMD), Military Service, and DAFA, currently leading the development and acquisition of capabilities and services across the Department including for use across the DoD Information Network. It delivers critical warfighter IT capabilities quickly and efficiently across the Department including provision of foundational worldwide IT transport infrastructure for the DoD and mission partners. I believe that DISA is in a key position to gather, coordinate and understand the pressing needs of DoD in all phases of the acquisition lifecycle and will continue to lead the department in the development and delivery of cutting-edge technology.

Congress enacted legislation directing that the National Security Agency's Cybersecurity Directorate conduct and support cybersecurity market research, testing, and acquisition across the Department of Defense. If confirmed, what actions would you take to ensure that this legislation is properly implemented?

If confirmed, I would ensure the roles and responsibilities are assigned to NSA and promulgated in Department policies. I would also ensure that DoD maintains a program to improve acquisition of cybersecurity products and services consisting of market research, testing, and expertise transmission, or augments to existing programs, to improve the its evaluation of cybersecurity products and services.

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?

Software systems are incredibly complex "systems of systems." Understanding the composition of software through a software bill of materials is a mandatory first step in understanding and either mitigating or consciously accepting a degree of cybersecurity risk. It also is a prerequisite for responding to newly-discovered vulnerabilities to determine what software in our inventory are affected and need immediate attention. If confirmed, I will drive Department-wide policy and establish timely guidance for generating, ingesting, and analyzing these software bills of materials.

As a co-chair of the Defense Business Council, what are your plans for using the annual Title 10 Section 2222 certification requirements to limit funds available to programs that, for example, don't comply with the Business Enterprise Architecture or with the Department's auditability requirements?

The Department plans to utilize an IT portfolio management process to optimize business systems and meet performance requirements, maintain pace with technological advancement, and eliminate unnecessary costs and vulnerabilities. The Defense Business Council will rely on the annual certification process to enforce portfolio management

decisions and ensure that business systems and their associated budgets align with DoD modernization objectives. If confirmed, I would provide active oversight of and involvement in these processes.

If confirmed, how would you plan to continue DOD's efforts to update its Business Enterprise Architecture while also working to better integrate the business architecture with the department's IT Architecture?

If confirmed, I would ensure that the Business Enterprise Architecture and the IT Enterprise Architecture are integrated into the DoD IT Portfolio Management process in order to provide the functional descriptions of the business and information enterprise necessary to achieve modernization and efficiency objectives. This will enable the DoD to assess current business systems and IT infrastructure and services, identify gaps, overlaps, and vulnerabilities, thereby informing investment decisions.

There have been a number of recent and sometimes public disagreements on how DOD components approach technology modernization, of which culture transformation is a critical element. What is an actionable strategy towards working with entrenched interests and practices to accelerate modernization? What does success look like in one, three, five year horizons?

If confirmed, ensuring that the Department modernizes the way it delivers software would be among my top priorities. Transforming from an environment where software deliveries are measured in years to one where deliveries are measured in minutes requires significant, deliberate change to our business processes, policies, workforce, and technology. This transformation demands a coordinated effort to reimagine today's environment and to rapidly address the challenges inherent in our current ways of acquiring, testing, securing, and deploying software. To that end, I understand that a DoD Software Modernization Strategy, developed by the DoD CIO, the USD(A&S), and the USD(R&E)—and built upon the already released DevSecOps Strategy Guide—will be published soon. This strategy defines the approach to accelerating the DoD enterprise cloud environment, establishing a Department-wide software factory ecosystem, and transforming DoD processes to enable technology resilience and agility.

The Department only recently migrated to Microsoft 365, with a mandatory shutdown of the Commercial Virtual Remote capability in June of 2020. As a result of this transition, DOD has lost a significant amount of collaboration capability with external organizations, including the congressional oversight committees. What is your plan to rectify these technical challenges such that interoperability with external organizations improves?

The DoD CIO office spearheaded the deployment of capabilities that have maximized DoD365 offerings with more enhancements from Microsoft being implemented in the environment. Today DoD can conduct meetings and have individual chats via Teams with any organization, to include communication within and external to the Department. The DoD CIO office authored and delivered a guide to assist our partners in enabling

these capabilities. If confirmed, I will ensure DoD CIO continues to work with Microsoft to prioritize capabilities in order to maintain commercial parity in the more secure environment offered by DoD365, all the while remaining in close coordination with other stakeholders across the enterprise.

Science, Technology, and Innovation

What are the key technologies that DOD should be supporting through research and development funding and procurement activities that will contribute to the effective execution of information systems modernization?

I believe that AI remains a cornerstone technology in our competition with China. Effective information system modernization will certainly benefit from advances in AI and machine learning. Adoption requires an ecosystem where cutting-edge commercial innovations and models can be installed, explored, and evaluated without fear of operational impact. Synthetic representational data must be supported in order to sit side-by-side with industry and work unencumbered from controlled unclassified information (CUI) and classification concerns. If confirmed, I would work closely with the Director of the JAIC, USD(R&E), and others to ensure DoD pursues a leadership position in the research and development of enabling AI-empowered and validated Zero Trust architectures. I would also advocate for technologies that advance and increase network bandwidth, such as through the integration of additional low-earth orbit (LEO) satellite communications to further compliment terrestrial capabilities. As network traffic continues to increase, I believe that more research into improving data compression algorithms would greatly benefit the information enterprise.

What do you see as the most significant challenges (e.g., technical, organizational, or cultural) to successful development of the key technologies for which the CIO bears significant responsibility?

The DoD CIO is responsible for information technology (IT), including NSS and defense business systems (DBS), information resources management (IRM), and efficiencies. Just by virtue of its size and complexity, the Department faces challenges in making large-scale changes at the enterprise level in areas such as adapting current systems, workflows, and data to work with modern technology frameworks such as Zero Trust and development, security, and operations (DevSecOps) frameworks. If confirmed, ensuring success against these challenges would be among my top priorities.

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

With the DoD DMS, I believe the Department is committed to properly focusing, integrating, and synchronizing key technology areas in cybersecurity, AI, cloud, and command, control, and communications. This strategy remains highly relevant, complementing the Department's long-term investments in AI that will enhance the

foundation of US defense capabilities relative to China and others. In my view, we already have seen the impact of the DoD DMS in the digital transformation strategies published by the Military Departments and DAFAs. If confirmed, I would use the DoD CIO's budget certification authorities to ensure the Department's IT and cyberspace activities budgets are sufficient to improve business platforms and improve joint warfighting.

If confirmed, what efforts would you undertake to identify new technologies developed commercially by the private sector and apply them to national security and warfighter purposes?

I believe that industry outreach is critical in this area. The Department has seen success, for example, in the Air Force's curated "Ask Me Anything" sessions with industry, and a desire from industry to directly offer feedback on DoD DevSecOps reference designs. If confirmed, and in close coordination with other stakeholders such a USD(A&S), USD(R&E), and the Military Departments, I would foster forums where industry can directly engage with the DoD and offer feedback to highlight areas where innovation is occurring. Strengthening relationships with the venture capital industry to create communication channels is another mechanism the Department could consider for more rapid identification of new technologies under development.

What responsibilities does the CIO have within the Office of the Secretary of Defense with respect to planning and directing the research and development of new, advanced information technologies?

The DoD CIO is the senior advisor to the Secretary of Defense for IT, including NSS and DBS, information resources management (IRM), and efficiencies. The DoD CIO advises the Defense Acquisition Board, Defense Space Council, Cyber Investment Management Board, Cyber Council, Defense Innovation Board and serves as the chair of the Committee on National Security Systems. I believe that addressing the Department's needs for research and development of new technologies requires ongoing collaboration. If confirmed, I will establish close working relationships and collaborative engagements with my peers to more effectively address the Department's research and development priorities. Additionally, the CIO should maintain a close relationship with USD(R&E) leadership to provide inputs on enterprise technology requirements and receive feedback on cutting-edge opportunities for further exploration.

Given the leading role of commercial industry in developing cutting edge information technology, what is the CIO's role in identifying and adapting key commercially developed technology for the Department?

The DoD CIO should ensure open lines of communication with commercial engagement and open up new opportunities for industry partners to deliver new innovations and technologies to address DoD mission needs. The Department continues to make significant strides in its ability to leverage nontraditional partners and commercial solutions.

What are the major emerging technologies and software development practices that you believe will have the greatest effect on the success of the Department's information enterprise into the future?

I believe that the speed that emerging technologies appear, mature, and impact operational environments is accelerating, and ubiquitous adoption of both cloud and DevSecOps enables success in tomorrow's information environment. Its greatest effect could come from unleashing the creativity of our civilian and military workforce, moving beyond the pockets of innovation that exist today to a widely-accessible ecosystem. This is fundamentally important because it enables junior officers and civilians, who are digitally savvy and extremely innovative, easy access to virtual enclaves with appropriate cybersecurity guardrails.

Budget Review and Standards-Setting Authority

Section 909 of the NDAA for FY 2018 empowered the DOD CIO 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 experience, how has this budget review and certification authority been used to shape the modernization and prioritization of cybersecurity and information technology infrastructure? If confirmed, to what investments and objectives would you envision this authority being best put to use?

The DoD CIO budget review and certification authority has been invaluable in helping shape and influence proper investment in IT and cybersecurity capabilities that are critical to supporting the NDS and the DoD DMS.

If confirmed, I will use this authority to ensure that the Department resources critical IT and cybersecurity investments that support the NDS, DoD DMS, and emerging requirements such as Zero Trust architecture, 5G technologies, cloud computing, and enterprise solutions.

What actions would you propose to take, if confirmed, to ensure that directives, policies, and standards originating from the Office of the DOD CIO 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 DOD Components' adherence to your directives?

If confirmed, I will work closely with the Military Department and DAFA CIOs to ensure they understand and are consistently implementing DoD CIO policies and directives. I will also use existing DoD governance forums, such as the Council on the Oversight of the National Leadership Command, Control, and Communications System; PNT Oversight Council; Command, Control, and Communications Leadership Board; CIO

Resources Board; and Digital Modernization Infrastructure Executive Committee to support my oversight responsibilities. Finally, I will also continue to leverage the budget review and certification authority that Congress has provided to ensure compliance with DoD CIO policies and directives.

Cybersecurity Architecture

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

DoD is a large organization that executes the budget in a decentralized fashion to achieve DoD-wide objectives in support of the warfighter. I believe that synchronization of those decentralized activities remains a key challenge. The Cybersecurity Reference Architecture enables organizations to align cybersecurity needs, goals, objectives to better integrate policies and acquisitions. Additionally, consistent application of the Cybersecurity Reference Architecture promotes adherence to common approaches and reuse of known, secured design patterns to repeatedly instantiate standardized, interoperable, and consistent solutions.

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?

In my view, the perimeter, network lawyer, and endpoint capabilities and DoD in-depth approach to cybersecurity has protected Department resources against the relatively unsophisticated tradecraft of the past. However, against well-resourced adversaries of increasing sophistication and insider threats, I believe DoD needs to do better. If confirmed, I would ensure the Department moves to a data-centric, Zero Trust concept based on micro-segmentation to better protect critical networks and information that will allow cyber defenders to detect and defeat advanced persistent threats (APTs).

In the wake of multiple severe cybersecurity breaches across industry and government organizations, DOD's stated goal is to accelerate adoption of "Zero Trust" architectures and capabilities.

How should the transition to a "Zero Trust" architecture affect the Joint Regional Security Stack program for both unclassified and classified networks, and the Department's Internet Access Points?

I believe that the transition to Zero Trust will evolve the Department's approach with the Joint Regional Security Stack (JRSS) deployments. The JRSS Program Management Office is planning to phase out JRSS, but will continue to maintain the 15 NIPRnet Joint Regional Security Stacks that supports approximately 1.5 million users until phase-out activities are complete. I understand there will be no deployment of JRSS on the SIPRnet due to DISA's implementation of its new "Thunder Dome" Zero Trust initiative.

What are the most important features of the "Zero Trust" Architecture that should be fielded over the next several years? Does the Department have approved plans and resources to achieve this objective?

The DoD Zero Trust Reference Architecture was publicly released in May 2021 and is being incorporated into the Department's Cybersecurity Reference Architecture. In response to the Executive Order 14028 on Improving the Nation's Cybersecurity, the Department released the initial Zero Trust Plan in July 2021. This plan will be continually edited and updated. I believe the most important features of the Zero Trust Architecture that will be fielded are end-point security technologies and an enterprise ICAM solution.

The Military Departments, the Defense Agencies, and the combatant commands are migrating to standardized cloud-based capabilities provided by Office 365. However, only the Navy is acquiring the set of comprehensive cybersecurity applications and capabilities available as options under this program. These cybersecurity capabilities are integrated and interoperable, and enable automated orchestration of security operations. These capabilities are supported by artificial intelligence, and meet "Zero Trust" Architecture goals.

As DOD has been unable to achieve an integrated, interoperable, and automated security enterprise through decentralized acquisition of commercial products, do you intend to consider mandating that all DOD Components acquire and implement a standardized set of capabilities through the M365 program that would enable that goal?

The Department is steadfast in its commitment to advance Zero Trust capabilities across all facets of its Information Enterprise. While the Navy's decisions to pursue a holistic solution from a single vendor meets their individual requirements, the DoD CIO, in partnership with USCYBERCOM, established a process for a cybersecurity baseline for DoD365 and minimum viable products to be tested by red teams, under the direction of DOT&E, to inform decision-based outcomes on both cybersecurity and affordability for the DoD365 cloud environment. Additionally, the DoD CIO office is in the process of establishing a Zero Trust Portfolio Management Office that will provide strategic guidance and oversight to ensure the Department adopts Zero Trust principals appropriately and in a timely fashion. This portfolio management office is a first major step to bring synergy and strategic oversight to a new and sophisticated cybersecurity architecture for the entire Department at scale.

Does the DOD CIO have the authority to issue such a mandate, in your view?

In my view, DoD CIO indeed maintains the authorities for such a mandate. Current statutes (Title 44, Sec 3544) grant the DoD CIO authority to establish and enforce standards across all of DoD, to include the Military Departments and DAFAs for capabilities to operate on defense networks. Similarly, DoD CIO responsibilities codified

in Section 142 of Title 10 provide the DoD CIO with statutory authority over Military Department and DAFA procurements of information technology-based capabilities to ensure compliance with Department-wide standards established by the DoD CIO. Those authorities provide the basis for any mandates the DoD CIO may establish.

Are Joint Force 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? If confirmed, what would you see as the next logical steps going forward in this regard?

JFHQ-DoDIN serves to integrate, synchronize and direct the cyber activities of different DoDIN areas of operation—across the Services and DISA. The scope and scale of the information cyber operations and security organizations need to perform their duties is vast and requires automation, big data analytics, and visualization to reach their full potential. The Department has been making significant investments to accelerate digital modernization, and are working towards real-time direction and orchestration in all areas. If confirmed, I would work with General Nakasone at USCYBERCOM to conduct a holistic assessment of our DoDIN cyber command and control capabilities to ensure our ability to accurately and continuously assess the Department's cyber readiness posture while improving the ability to respond in near real-time.

How is the Department planning to implement and employ microsegmentation and software defined networking technologies 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?

DISA is leading the efforts for the Department in actively developing and fielding Software Defined Networking (SDN) capabilities within its backbone, including efforts for automation of service delivery, and configuration normalization across backbone, data centers and managed local area networks. DISA is engaged in the development of Software Defined-Wide Area Networking (SD-WAN)-enabled service delivery nodes to leverage modern technologies and delivery mechanisms. Project Thunder Dome will incorporate SD-WAN enabled application aware routing on existing, fielded Defense Information System Network (DISN) core infrastructure. DISA is actively working with DoD components to enable SD-WAN mission platforms to seamlessly integrate into larger DoD communications capabilities.

The Military Departments, the Defense Agencies, and the combatant commands are migrating to standardized cloud-based capabilities provided by Office 365. However, only the Navy is acquiring the set of comprehensive cybersecurity

applications and capabilities available as options under this program. These cybersecurity capabilities are integrated and interoperable, and enable automated orchestration of security operations. These capabilities are supported by artificial intelligence, and meet "Zero Trust" Architecture goals.

If confirmed, what policies would you plan to enact to help limit DOD's attack surface and vulnerabilities – especially to persistent threat agents?

I believe that implementing Zero Trust requires rethinking how the Department utilizes existing infrastructure to implement security in a simpler and more efficient way while enabling unimpeded operations. If confirmed, I will adapt lessons-learned from pilot efforts across the Department to move DoD towards the rapid adoption of Zero Trust and SDN. It is my understanding that the Navy's efforts have been coordinated with the office of the DoD CIO and are being used as a pathfinder to directly influence the Department's cybersecurity requirements, policy, and architecture.

Please share your thoughts on how DOD is addressing (or planning to address) the requirements for cybersecurity set forth in Executive Order 14028, Improving the Nation's Cybersecurity? For example, among other things, DOD in collaboration with other agencies, including the Department of Homeland Security, is to jointly develop procedures for ensuring that cyber incident reports are appropriately shared among agencies. Can you provide us with the status of the procedures or any of DOD's activities related to the cyber EO?

On July 7, 2021, the DoD and DHS signed a memorandum of agreement (MOA) to establish formal procedures to immediately share DoD Incident Response Orders or DHS Emergency Directives and Binding Operational Directives. I believe that sharing this information will raise the enterprise baseline cybersecurity posture across the entire federal government. DoD has also assisted with providing procedures for ensuring cyber incident reports are promptly and appropriately shared among agencies, drafted a national security memorandum (NSM) to improve the protection of NSS across the federal government, and holds a chair on the Cyber Safety Review Board.

Please identify the report(s) and frequency of reports you receive on DOD's cybersecurity posture. Do you believe that these report(s) you are sufficient? Overall, what grade would you give DOD's cybersecurity posture?

The Department has used three scorecards to assess the DoD's cybersecurity posture, which include the monthly Cybersecurity Hygiene Scorecard (CHS); quarterly Top 10 Scorecard; and monthly Network Cybersecurity Accountability Scorecard (NCAS). I believe these reports are sufficient and, if confirmed, would ensure the Department continues a laser focus on maintaining a proactive cybersecurity posture.

Is it possible for DOD controlled unclassified information (CUI) information systems to have more than 50 percent of applicable security controls found to be "non compliant" and still allowed to operate on the DODIN? Is it possible for DOD

CUI information systems to have less applicable security controls found to be "compliant" than a system that does not have CUI? If the answer to either of these questions is affirmative, and if CUI is supposed to be more important to protect than publically-reliable information, why has DOD CIO not established minimum security controls for CUI systems?

Yes, it is possible. The Federal Information Security Modernization Act (FISMA) mandated the Risk Management Framework (RMF) process and does not establish compliance requirements for cybersecurity, but focuses efforts on managing cybersecurity risk in systems. I understand that the Department has a number of non-traditional systems that process CUI that, when compared to the security control baseline of a traditional IT system, have a high rate of non-compliant controls. The DOD is working with the National Archives and Records Administration (NARA) on ensuring all systems manage the cybersecurity risk to CUI data while meeting all requirements through a policy memo titled, "Requirement for Applying Baseline Controls for Controlled Unclassified Information Systems."

What is your perspective on harmonizing DOD CUI standards to support a whole-of-government approach with NIST 800-53, the recent Executive Order on Zero Trust, and other standards?

The DoD follows the security standards for CUI as established by the Executive Order. DoD CIO is ensuring systems processing CUI data meet these standards through a policy memo titled, "Requirement for Applying Baseline Controls for Controlled Unclassified Information Systems." DOD requires all systems processing CUI data meet the moderate-moderate threshold. If confirmed, I would support continued efforts to reinforce the whole of government approaches to harmonizing CUI standards. However, DoD has a number of non-traditional systems that process CUI (weapons systems, control systems, etc.) and the cybersecurity risk to CUI in these types of systems is fundamentally different. I believe that flexibility to manage cybersecurity risk is needed for these unique use cases.

There are currently legislative proposals to require industry to report cyber incidents to federal government. DOD has had a cyber incident reporting requirement for years (DFARS 252.204-7012). To what extent has this cyber incident reporting requirement provided DOD any benefits? What does DOD do with this information? What challenges has it had in ensuring this acquisition requirement is complied with?

The DoD DIB Collaborative Information Sharing Environment (DCISE) serves as the single DoD focal point for receiving all cyber incident reporting affecting unclassified external networks (i.e., contractor or other government agency). Information shared between DoD and DIB Cybersecurity (CS) Program participants increases the nation's knowledge of growing cyber threats, resulting in a greater capability to respond to and mitigate these risks. Reporting information is then used to identify and respond to adversary activity, identify vulnerabilities, provide mitigation and remediation strategies,

and help improve overall network defenses of USG entities and DIB CS Program participants.

Defense Industrial Base (DIB) Cybersecurity

DOD CIO is supposed to be chairing the DIB Cybersecurity Executive Committee. How active is this committee? How often does it meet? What specific accomplishments has it achieved in the last 2 years?

As cybersecurity has matured within the Department and across US Government, the DIB Cybersecurity Executive Committee's mission has been addressed through the Government Coordinating Council (GCC). The GCC brings key leaders in cybersecurity across multiple USG components together, to collaborate and discuss all threats facing the DIB and USG, in addition to strategies to protect the warfighter. The GCC has a complimentary Industry council, called the Sector Coordinating Council (SCC), which discusses the same challenges from the prospective of Industry, and then convenes with the GCC to discuss areas of mutual concern and strategize on a way forward. Both councils meet monthly and additional meetings are scheduled as necessary. Two specific accomplishments include driving the mitigation and remediation strategies for SolarWinds and Microsoft Exchange vulnerabilities.

The CMMC framework does not allow contractors to use corrective action plans (a.k.a. POA&Ms) for security controls that are applicable to the system but are found to be non-compliant. However, DOD relies extensively on POA&Ms.

In your opinion, should DOD establish a requirement for industry that it does not practice itself?

The DoD often has requirements in place that exceed industry practices, and industry often mirrors DoD requirements. I understand that DoD is reviewing CMMC, including its exclusion of POA&Ms, for the barriers to doing business with DoD that it may establish. If confirmed, I will quickly learn about the results of this review and help assess whether there should be areas for greater symmetry for POA&Ms and similar practices between DoD and industry.

Adoption of Commercial Cloud Services

The single-award acquisition strategy pursued in the first phase of the Joint Enterprise Defense Infrastructure (JEDI) initiative was intended to enable the Department to rapidly move workloads and data to an enterprise cloud without delays stemming from the need to compete each specific migration in task order-type multi-award contracts. This strategy was upended by continuous litigation, preventing DOD from making any significant progress on cloud migration. Now, years later, DOD plans to make multiple awards for general purpose enterprise clouds.

How does the Department now plan to allocate cloud migration workloads across multiple vendors rapidly? Will each discrete transition be competed among the multiple vendors receiving awards in the Joint Warfighter Cloud Capability program? Has the Department taken any steps to ensure that vendors fully understand the JWCC requirements?

The Department plans to have multiple cloud service providers compete for mission owner cloud requirements at the task order level by using streamlined, fair opportunity ordering procedures. I understand that a JWCC Ordering Guide is in development and will detail how to order cloud services from the JWCC Indefinite Delivery/Indefinite Quantity (IDIQ) contract. With this, the Department will be able to leverage an automated provisioning tool to expedite cloud resource allocation and allow mission owners to provision cloud resources within days of the task order award. Each mission owner will be able to acquire cloud services to meet their specific mission needs in accordance with the Federal Acquisition Regulation (FAR). The Department has taken measured steps to ensure that the U.S.-based hyper-scale cloud service providers (CSPs) fully understand JWCC's requirements. Initially, a Pre-Solicitation Notice that outlined high-level JWCC requirements was posted on SAM.gov. Next, the Department held multiple meetings with major U.S.-based hyper-scale CSPs to discuss their services and capabilities and determine how they aligned with JWCC requirements and timelines. Finally, following receipt of the solicitation, the vendors will be able to ask any clarifying questions about the requirements before final proposals are due to the Department. I further understand that the Department is confident these measured steps will help vendors fully understand the requirements.

Commercial enterprise cloud providers have balked at requests from DOD officials to evaluate, including through Red Team testing, the security of their cloud provisioning, control plane, and hypervisor. The Office of the Director of Operational Test and Evaluation, in particular, has regularly voiced concerns that DOD has not generally been permitted to evaluate for itself whether these clouds are sufficiently secure.

What are your views on the need for DOD to be able to assess the foundational security of the commercial clouds on which DOD will increasingly depend?

I believe that it is critical that the DoD assesses the security of commercial cloud environments. Penetration testing is an existing requirement of the Cloud Computing Security Requirements Guide, which all cloud contracts are required to follow, per DFARS clause 252.239-7070. If confirmed, I welcome the opportunity to work with the DOT&E to strengthen and enhance our existing cloud cybersecurity policies to explicitly allow increased testing. DoD CIO recently collaborated with the testing and evaluation community to ensure their requested language for enabling DoD testing of cloud vendors is included in JWCC requirements. As the DoD transitions more workloads to the commercial cloud, it must ensure that it maintains the right level of assurance that DoD data is protected properly through the ability to perform cybersecurity assessments of commercial cloud infrastructure.

When DOD initiated the JEDI program, DOD officials stated that a single initial award was sensible because: (1) the DOD workforce would have great difficulty in handling the technical integration challenges involved with multiple cloud vendors; and (2) interoperability and data portability across clouds was not mature in the commercial cloud industry.

Are you concerned that DOD personnel lack sufficient capacity and expertise to transition workloads to multiple clouds simultaneously?

Since the inception of the JEDI program several years ago, both the cloud ecosystem and the expertise of DoD personnel have evolved. Even so, it is my understanding that JWCC provides mission owners a great deal of flexibility—while they can transition their workloads to multiple cloud environments, they may also choose to pursue a single-cloud environment. Mission owners will make this decision based on their workforce expertise, mission, and operational requirements.

Has industry made significant progress on cross-cloud interoperability since JEDI was initiated?

The Cloud Native Computing Foundation (CNCF) is developing a broad range of open technologies and standards that enable organizations to build and run modern applications across public, private, and hybrid clouds. These technologies, such as Kubernetes, micro-services, and service mesh form the backbone of the Department's DevSecOps environments, as seen in the US Air Force's Platform One and Kessel Run.

In your view, what are the benefits and downsides associated with expediting the movement of DOD Components' data and networking functions to enterprise clouds?

As I learned firsthand in my experience leading the IC's IT ecosystem, cloud computing is a core component of a modern IT environment. It is critical to delivering enhanced DoD mission capabilities, expanding the use of AI and machine learning, and maintaining the Department's technical advantage. I agree that "Cloud Smart" rather than "Cloud First" is the correct strategy, which means that mission owners should rethink their approach to cloud by conducting inventories of their systems to determine which systems can move to the cloud and which systems should be decommissioned. This methodical, upfront work is necessary to build both the strategic implementation plan and associated resourcing strategy to re-architect their systems when migrating to the cloud, rather than preforming a pure "lift and shift" operation. Clouds provide a powerful foundation for modern applications but can be expensive and cumbersome when supporting older IT systems that have not been tailored to fully harness the power of the cloud environment.

Given the lessons from JEDI, a variety of cloud instances are proliferating across DOD. What is your perspective on harmonizing various implementations of cloud instances from different cloud service providers to standardize deployment,

information security posture, and cost management?

DoD continues to see consolidation of cloud contracts across its enterprise. Each of the Military Departments has created preferred contract vehicles, along with corresponding managed service provider organizations, to drive cloud migration and adoption. I believe that JWCC will provide a much-needed enterprise cloud solution through a multi-vendor, multi-cloud IDIQ contract. Moreover, JWCC will address the urgent, unmet cloud capability gaps needed to support JADC2 and the ADA Initiative. Regardless of cloud contract or cloud service provider, the DoD's overall goal in the move to cloud computing should be to make it as simple as possible for a mission owner to purchase, secure, deploy, and maintain their cloud workloads.

Artificial Intelligence

In your view, what are the major challenges facing the Department of Defense relative to its efforts to leverage artificial intelligence capabilities to support defense missions?

The DoD continues to face significant difficulty in recruiting, training, and retaining a skilled AI technical workforce that is familiar with how to develop, manage, and utilize AI-enabled systems. Beyond core technical expert staff, many communities within the existing DoD workforce require additional training to execute their existing functions in AI contexts. In addition to workforce expertise, the primary barriers to DoD AI adoption include technical debt across the IT ecosystem and challenges associated with data quality and availability.

The Joint Artificial Intelligence Center (JAIC) initiated the Joint Common Foundation (JCF) program. The price of entry for AI is large-scale computing infrastructure. Thus, it makes no sense for all the DOD Components seeking to develop AI applications to build such complex and expensive computing platforms. The JCF objective, therefore, is to provide common large-scale computing infrastructure, services, and applications to DOD Components so that they can rapidly apply their domain expertise to build AI solutions. There are multiple companies providing mature commercial platforms for this purpose. However, the JAIC appears to be pursuing a government-developed solution that could prove technically challenging, expensive, and time-consuming. Section 215 of S.2792, the Senate Armed Services Committee enacted version of the NDAA for FY 2022 would require DOD to acquire access to commercial platforms and services under part 12 of the Federal Acquisition Regulation for these purposes.

What are your views on the best approach to providing the infrastructure and services required to enable DOD Components to rapidly apply their domain expertise to develop AI solutions for their missions?

The Department must develop an enterprise approach in order to deliver AI solutions across multiple and diverse mission sets. To do this, it must use commercial, open source tools, and cloud computing environments.

At this point in the maturity of AI, there is not a single-set of infrastructure services that will meet DoD needs. DoD requires a combination of commercial cloud, on premise, commercial tools, and open-source tools that each target unique requirements across the functional communities. This is the set of needs the DoD's Joint Common Foundation (JCF) is filling. First, JCF integrates infrastructure and services from leading commercial providers. JCF is built on commercial infrastructure. This is available now to the Services, promulgating best practices and a centralized architecture that distributes capability throughout the enterprise. Second, the JCF effort is building a fabric between these commercial services and other DoD platforms to create a development environment that can support DevSecOps. This broad enterprise-wide approach will then support portability and integration of data and AI models to achieve true interoperability of data and insights at scale and ensures economies of scale and interoperability across the enterprise. If confirmed, I would work closely with the JAIC Director to continually evaluate the JCF approach, especially in light of new capabilities such as with JWCC.

The National Security Commission on Artificial Intelligence recently completed its work and published its findings and recommendations.

What specific Commission recommendations do you believe the Secretary of Defense and the CIO should implement?

While there are many outstanding recommendations in the National Security Commission on Artificial Intelligence (NSCAI) final report, there are 11 that I believe would do the most to transform DoD into an AI-ready institution, if implemented.

- Build the technical backbone
- Define a joint warfighting network architecture
- Train and educate warfighters for AI
- Establish AI and digital readiness performance goals
- Accelerate adoption of existing technologies
- Tailor and develop Test, Evaluation, Verification, and Validation policies and capabilities
- Strengthen the Responsible AI (RAI) ecosystem
- Develop and deploy AI-enabled defenses against cyber attacks
- Invest in priority research and development areas to support future military capabilities
- Promote AI interoperability and adoption of critical emerging technologies among allies and partners
- Improve AI coordination and interoperability between DoD and the IC

These NSCAI recommendations offer the greatest return on Department investment in broad-scale AI readiness.

If confirmed, what do you envision as the next steps in the process for Department use of machine learning and advanced statistical methods to improve its business,

maintenance, and management practices? What improvements could result from these efforts, in your view?

The wholesale integration of business, maintenance, and management practices is an important mission. I believe that Advana and its integration of AI-enabled capabilities is an early example of what is possible when AI is integrated into enterprise platforms. The DoD CIO is both a user of Advana and an advocate and enabler for enhanced enterprise use of this powerful capability through the incorporation of additional data sources spanning the enterprise.

In your view, 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?

Yes. The JAIC continues to implement methodologies for smaller and non-traditional innovation sources to leverage Department acquisition processes. Through consortium-based models like the Other Transaction Authority (OTA) called "Tradewind," and Blanket Purchase Agreement models for Responsible AI and AI Test & Evaluation, procurement barriers can be reduced. The Department maintains mature relationships with multiple universities and their laboratories today, and these partnerships should continue. Advancing technologies to meet critical national security needs through innovative academic and commercial partnerships is a key component of DoD's strategy.

How can the Department of Defense use procurement and research activities to shape the direction of commercial sector artificial intelligence efforts and create incentivizes for the production of technologies that can support defense missions?

The DoD is consistently collaborating with industry to leverage best practices and technological innovations. The JAIC is utilizing the OTA called "Tradewind" to drive AI innovation at scale and foster collaboration with small business and non-traditional companies. I believe that the integration of mature commercial technology into growing Defense systems is a critical pipeline that must be maintained. The Department continues to steer commercial efforts into use-cases through broad partnerships and sharing of Defense challenges in a variety of forums, and I understand these relationships are vibrant. New AI companies are proliferating rapidly, many of them specifically in response to DoD demand signals.

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

The DoD needs to adopt, scale, and deliver AI solutions to warfighters. These concepts, plans, and capabilities come from a variety of sources. Service AI efforts are integrated through Joint warfighting concepts, exercises, and requirements developed by the Joint Staff and CCMDs. A key component of this effort is the ADA Initiative, directed by the Deputy Secretary of Defense and led by a partnership including the JAIC, CDO, CIO, USD(R&E), JS J6, DDS, and others. Through ADA, the DoD will incentivize and

accelerate a set of global, open architecture data and process solutions that embed modern data management and analytics capabilities to automate business and warfighting workflows.

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 governance of AI is a critical enabler of the ethical and safe application of AI technology to DoD's warfighting missions. The AI Executive Steering Group ensures accountability throughout the Department. In addition, the Deputy Secretary of Defense has directed the implementation of a RAI ecosystem throughout the Department. This guidance reaffirmed the five DoD AI Ethical Principles and outlined the contours of RAI governance. Through this effort DoD will cement a culture of ethical and safe application of AI in the Department.

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?

DoD has deep and ongoing engagements with our allies and partners on AI, including in the area of standards and norms for the ethical and safe application of AI. For example, the JAIC has conducted bilateral and multilateral engagements with approximately 40 allies and partners. Nearly all of these engagements included substantive discussions of RAI, ethics, and sharing of good practices to enable AI readiness and interoperability among allies and partners. The Department's "AI Partnership for Defense" brings together 16 nations based on a common ethical framework and responsible outcomes. This is a dynamic and effective environment for shaping global understanding of responsible and ethical AI application. Similarly, the development of the DoD AI ethical principles involved deep collaboration with leading commercial technology organizations and public policy non-profits. The DoD continues to solicit the advice and expertise of both groups as it implements its RAI Strategy.

How are you integrating AI/ML capabilities into DOD's data architecture, and what investments do you think need to be made in order to ensure that decision-makers have the right information at the right time?

Maturing the unique, Service-specific infrastructures and architectures into an integrated enterprise is an essential element of DoD's warfighting effectiveness and global competitiveness. Current efforts span a scaled data environment, an integrated AI development fabric, AI Test & Evaluation, and AI applications at the CCMDs and at the tactical edge. Commanders and decision-makers across DoD require access to data and insights generated across components, domains, and network boundaries. Department AI/ML capabilities, and the investments made in them, only achieve their full potential through integration. This creates conditions necessary for implementing AI/ML capabilities at-scale. In my view, the Department needs to quickly and effortlessly

discover, access, and utilize data, compute, and services so that individual components can leverage these Department-wide resources to build AI capabilities.

Electromagnetic Spectrum Policy and Operations

Based on information gleaned from internal DOD assessments and Committee oversight activities, it would appear that the Department's electronic warfare posture is dangerously inadequate.

Under the electronic warfare implementation plan announced in August of 2021 the DOD CIO will assume the roles and responsibilities of the level 2 senior designated official under section 1053 of the FY 2019 NDAA, and will now be responsible for overseeing the implementation plan of a cohesive electronic warfare strategy DOD wide. What makes you qualified to assume these roles and responsibilities?

Achieving spectrum superiority in all domains is critical to U.S. national security. The 2020 EMS3 provides the strategic direction and oversight to address identified gaps in U.S. posture and generate results. DoD CIO is at the nexus of Department's EMS policies, strategies, and international and national engagement. As the PSA for EMS to the Secretary and the newly assumed roles and responsibilities, the DoD CIO will ensure enduring enterprise focus on EMS strategy. If confirmed, I will work closely with the Joint Chiefs of Staff (JCS) and other stakeholders to ensure that the implementation plan supports the operational needs of our military forces.

In a brief to congressional staff on August 5, 2021, five goals were outlined for the strategy and objectives of a cohesive DOD wide electronic warfare strategy. Please discuss each goal, what you envision to be the major hurdles associated with accomplishing each goal, and what you would do, if confirmed to overcome each such hurdle.

The EMS3's goals have a common hurdle. Historically, the Department has approached Electromagnetic Spectrum Operations (EMSO) in isolation. The Department has now focused on an enterprise-wide strategy to overcome the challenges caused by unique, isolated approaches. In my view, the Department now has the policy, governance, and people in place to address such challenges. The EMS3 sets DoD on a course to view EMSO in a more strategic and integrated manner. If confirmed, I will continue to drive this paradigm change.

The DOD CIO's selection as the senior designated official in the DOD for electronic warfare renders the CIO responsible for "establish[ing] process and procedures to develop, integrate, and enhance the electronic warfare mission area and joint electronic spectrum operations in *all domains across the Department of Defense*." If confirmed as the DOD CIO, you would be responsible for certifying that the overall budget for electronic warfare is adequate and integrated as follows—

"(A) The development of an electromagnetic battle management capability for joint electromagnetic spectrum operations.
(B) The establishment and operation of associated joint electromagnetic spectrum operations cells."

Do you believe the DOD is making adequate progress in a joint battle management capability for spectrum operations? If not, how can these efforts be improved, in your view?

In my view, the DoD CIO will rely heavily on the best military advice of the Vice Chairman of the JCS and Commander, US Strategic Command, who remain responsible for Electronic Warfare (EW) matters.

The Department continues to make strong progress in a joint battle management capability for spectrum operations. As the Department continues the Electromagnetic Battle Management (EMBM) development effort, it is balancing lethality and joint interoperability with fiscal responsibility. Additionally, to ensure the appropriate data gets to the tactical edge requires the DoD to establish an EMSO architecture that connects with all relevant stakeholders. If confirmed, I will ensure that these efforts continue.

Do you believe the DOD has successfully implemented joint electromagnetic spectrum operation cells? How can DOD's efforts in this regard be improved, in your view?

I believe that the DoD has successfully started to implement Joint EMSO Cells (JEMSOCs). Properly incorporating EMSO into operational plans and accounting for real-time activities requires the appropriate staffing of JEMSOCs in each CCMD. DoD is also evaluating the long-term home for EMSO responsibilities in the Department in accordance with FY21 NDAA Section 152 requirements.

To enable continued success, I believe DoD must ensure appropriate resource allocation, and that training requirements and that EMSO capabilities, such as EMBM, are developed and employed.

If confirmed, how do you plan to integrate with the combatant commands who will be responsible for executing the cohesive electronic warfare strategy you are responsible for?

If confirmed, the DoD CIO will continue to work directly with the Joint Staff as a co-chair of existing governance bodies. Many of the Department governance forums also include direct engagement with CCMDs as well, ensuring awareness of and advocacy for CCMD requirements.

On page 6 of the July 15, 2021, report entitled "Summary of Implementation Plan for 202 DoD EMS Superiority Strategy and Attached Roadmap," submitted to congress pursuant to section 1053(d)(3)(E), DOD stated: "[a]dditionally, the Implementation Plan

requires the Office of Undersecretary of Defense for Policy (OUSD(P)) to designate one of its Deputy Assistant Secretaries of Defense to advocate for and represent EMSO interests in OUSD(P)."

What assistance would you expect the USD(P) to provide you, if you are confirmed as the DOD CIO and vested with the authorities and responsibilities of the section 1953 senior designated official?

If confirmed, I would expect continued support from and close partnership with USD(P) in ensuring the EMS equities are captured in the Department's policy decision-making process.

If confirmed, how would you expect to influence the Defense Planning Guidance?

If confirmed, I would look forward to influencing the Defense Planning Guidance (DPG) to elevate investment in capabilities that would digitally modernize the Department's EMS Enterprise; leverage more agile, adaptable, and survivable EMS capabilities; establish secure, responsive and integrated EMS infrastructure; and further advance live, virtual, and constructive (LVC) capabilities. Altogether, these initiatives will enable enhanced testing and training in representative EMS environments against realistic threats.

DOD conducts an annual Northern Edge exercise to assess the Joint Force capabilities in an electromagnetically contested spectrum environment.

In your view, how will this exercise influence your actions and decisions as the senior designated official? If confirmed what actions would you take to improve capabilities to provide realistic threat capabilities to the joint force?

If confirmed, in coordination with the JCS, I would leverage the Joint Pacific Alaskan Range Complex for exercises that include training, testing, and developing advanced electronic warfare capabilities in a realistic environment.

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

The DoD has reorganized, improved governance structures, and implemented new policies to best ensure the Department can compete with near peer adversaries in an increasingly congested, contested, and constrained environment.

The DoD faces two main challenges, the first is outdated regulations and policies that have not evolved with the current environment. Second is the drive to share or vacate EMS to enable commercial mobile broadband technologies. While I absolutely support enabling commercial access to spectrum, the increasingly congested spectrum ecosystem is a challenge that, if confirmed, I would need to address.

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

All warfare domains, to include the EMS, are challenged by peer and near-peer adversaries. Recognizing US reliance on the EMS, our adversaries have spent decades studying, investing, and implementing policies, capabilities, and procedures with the absolute focus of gaining military advantage over US forces. These adversaries are developing and fielding advanced technology that targets US capabilities across the spectrum.

Through implementing the DoD EMS3, the Department is working to develop a spectrum enterprise that is fully integrated, operationally-focused, and designed for great power competition.

Please define your view of the appropriate sharing of spectrum between the DOD and non-federal users.

I believe that DoD has been a national leader in thinking broadly about new solutions and has already participated in several spectrum-sharing initiatives. These have contributed to US leadership in enabling the use of mid-band spectrum for commercial 5G. Acknowledging that progress, I also believe that spectrum *sharing* (vice spectrum vacating) now needs to be the new normal. Such an approach offers federal and non-federal users a new paradigm by allowing simultaneous usage of a specific frequency band in a specific geographical area and time by a number of independent entities where harmful electromagnetic interference is mitigated.

To date, federal policymakers have made unprecedented amounts of spectrum available for commercial use across large, contiguous spectrum ranges. Now, I believe the DoD must also develop spectrum sharing policies that enable the most efficient use of spectrum while still protecting and prioritizing mission critical functions.

What are your views regarding the potential sharing of spectrum for both federal and non-federal bands? Do you believe the Department can adequately share spectrum in the band of 3.0-3.45 MHz and what actions must be taken, and by whom, before such sharing can occur? Please explain your answer.

I believe that sharing of spectrum for both federal and non-federal bands is the new normal. DoD is pursuing a range of possible solutions that improve access for military missions and enhance US economic competitiveness for 5G and other advanced technologies.

As such, I believe the Department can share the 3.1-3.45 GHz band. Technical and operational feasibility assessments are required to identify the best sharing framework for this band. These feasibility assessments will identify the amount of spectrum that could be made available, regulatory requirements needed to protect incumbent military operations, and the associated costs and timelines for implementation.

Upon completion of the assessments, I believe a whole-of-government approach is required to determine which sharing framework best meets the nation's needs.

Is the Department investigating and investing in technologies to enable: (1) simultaneous use of commercial wireless networks and DOD military systems in the same spectrum; (2) simultaneous transmit and receive capabilities; and (3) continuous operations through very high levels of interference and jamming? Could such technologies resolve competing demands for spectrum and help to meet the Department's EMSO warfighting objectives, in your view?

Yes, the Department is investing in and investigating these types of cutting-edge technologies for inclusion in future military capabilities. I believe they hold great promise for both addressing competing demands for spectrum, which are increasing across all users, and helping to meet the Department's EMSO warfighting objectives.

The vision of the EMS3 is the ability of our forces to enjoy freedom of action in the electromagnetic spectrum, at the time, place, and parameters of our choosing. To facilitate this outcome, I would, if confirmed, ensure that DoD CIO continues to partner with OUSD(R&E) and OUSD(A&S) to develop and integrate these types of capabilities to meet the warfighter's current and future requirements.

How will you help ensure that DOD's execution of the spectrum IT modernization requirements in the FY21 NDAA are successfully implemented? In particular, how will you ensure that DOD's IT systems collect the necessary information to facilitate spectrum sharing where possible and are designed in such a way to enable rapid or real-time processing of spectrum assignment adjustments?

If confirmed, I will ensure that DoD CIO continues with development and implementation of a plan to successfully modernize and automate the spectrum IT infrastructure, per the requirements in Section 9203 of the NDAA for FY21. This modernization effort will be key to advancing agile spectrum management operations. I understand the intent is to develop a common spectrum IT architecture; improve data collection and aggregation; standardize analytical tools and methodologies; increase spectrum situational awareness, spectrum access and sharing; and establish integrated and standardized automation interfaces.

Positioning, Navigation, and Timing (PNT)

In your view, what are the major threats and technological challenges facing the Department of Defense as pertains to its positioning, navigation, and timing (PNT) programs and capabilities?

In my view, the Department relies heavily on the Global Positioning System (GPS) and our adversaries are well aware of this dependence and have developed extensive capabilities to deny our access to GPS. Additionally, while GPS has been critically

beneficial over the last several decades, the PNT Enterprise is complex and the DoD should develop and field alternates and complements to GPS to address known threats.

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 very serious existing and anticipated threats to the system. Upgrades to GPS and user equipment are being acquired, but significant vulnerabilities remain and the expected implementation time is significant. Congress has mandated near-term measures to field more resilient alternative PNT solutions to complement and augment GPS.

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 my view, the Department is aware of the vulnerabilities of GPS. I am a strong advocate for the Department to identify, invest in, and field alternate and complementary sources of PNT to enhance PNT now and in the future. In June 2021, the Department submitted a report on progress on alternative PNT capabilities in response to a tasking in Section 1611 of the FY 2021 NDAA. While a "one-size-fits-all" solution is not feasible, the Department has made significant strides in fielding alternate and complementary capabilities in programs such as the GPS-Based Positioning Navigation and Timing Service (GPNTS), the Mounted Assured Positioning, Navigation and Timing System (MAPS), and the Dismounted Assured Positioning, Navigation and Timing System (DAPS). While progress is slower in the air domain, the Air Force is pursuing an open architecture-based Resilient-Embedded GPS/Inertial (R-EGI) that will enable the integration of existing capabilities and new PNT alternatives. If confirmed, I would continue to champion development of modernized receivers and fielding of the alternate PNT sources they will process to provide PNT resilience to the Joint Force.

What is your assessment of DOD's ability to implement a timely strategy to provide Military Grade User Equipment (MGUE) navigation cards to the wide array of platforms and weapons the Department uses and how can DOD efforts in this regard be improved?

It my understanding that DoD CIO is working closely with the Joint Staff, Services, and USD(A&S) to monitor program progress and ensure that MGUE development and fielding have required priority and associated resources. Longer-term, I believe that implementing a Modular Open System Approach (MOSA) will enable faster and more agile integration of additional GPS and alternative and complimentary PNT sources.

What is your assessment of DOD's progress in providing alternate means for PNT to DOD platforms and weapons? If confirmed, what actions would you recommend be taken to accelerate DOD efforts in this regard?

I believe that the Department is making significant strides in testing and implementing effective alternate PNT capabilities. I support these efforts and, if confirmed, I will continue to push these efforts forward.

What is your assessment of the effectiveness of the PNT Oversight Council authorized under section 2281 of title 10 U.S. Code? If confirmed, what actions would you take to improve the Council's effectiveness?

In my view, the PNT Oversight Council is effective in executing governance and providing oversight of the DoD PNT Enterprise. The Council has driven development and fielding of more resilient GPS and is now also focused on the delivery of alternative and complimentary PNT solutions. If confirmed, I would support continuation of these efforts as well as the incorporation of GPS and PNT data into the Advana platform, enabling enhanced tracking and oversight of the full scope of efforts across the Department.

Fifth Generation Wireless Networking (5G)

5G wireless networks are the foundation for future industrial transformations that will power the world economy via applications such as vehicle autonomy; the Internet of Things; telemedicine; smart factories, ports, and warehouses; and smart cities. It is widely recognized that U.S. national security and economic well-being would be jeopardized if Chinese companies such as Huawei dominate 5G global wireless infrastructure. DOD has robustly funded research and development in 5G technology and in the applications that will be enabled by the speed, low-latency, and capacity of 5G networks. Although the Office of the USD(R&E) is currently managing DOD's 5G program, Congress directed the Department to begin preparations to transfer that responsibility to the CIO as projects and technologies mature. The Committee is concerned that budget reductions would prevent the achievement of these objectives. Accordingly, the Committee has recommended authorization of an additional $100 million for 5G-related technology in FY 2022.

In your view, how would significant reductions in funding for DOD's 5G program affect U.S. industry's ability to compete with Huawei in the global 5G market?

In my view, significant reductions in funding for DoD's 5G programs would curtail the progress the Department has made in reducing Huawei's influence in establishing the technical specifications for commercial 5G user devices, network components, and cellular services, as well as significantly slow the development of verified and secure applications of 5G Technology in the transport layer of the department's mission-critical voice and data communications.

In your view, how would budget reductions in the near term affect the ability of the DOD CIO and the Military Departments to transition successful 5G technology development projects?

In my view, budget reductions in the near term would significantly hamper the activities of the CFT legislated in the FY21 NDAA to oversee the implementation of the strategy developed under section 254 of FY20 NDAA. This strategy was coordinated across all relevant elements of the Department and will drive the adoption of commercially

available, next-generation wireless communication technologies, capabilities, security, and applications by the Department and the DIB. If confirmed, I will continue to work with my counterparts in USD(R&E) to ensure a successful transition of these responsibilities.

What are your views on the importance of rapidly maturing technologies to create modular 5G network architectures based on open standards, and to virtualize network functions through software, in enabling U.S. companies to compete with Huawei globally? Does DOD have a role to play in achieving that objective?

I believe that modular 5G network architectures, based on open standards and software-enabled virtualized network functions, are critical to promote the development and deployment of user devices and network components manufactured by US and allied nations' industrial bases, in lieu of Huawei. I understand that DoD is promoting these modular 5G network architectures through participation in international Standards Development Organizations, inclusion of modular 5G network architectures in the DoD's 5G pilot experimentation efforts, and the development of supply chain standards and acquisition tools for the deployment of 5G technology across the Department. If confirmed, I would sustain focus and momentum on these activities.

Command, Control, and Communications

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?

In my view, modernization of our existing C3 systems is critical to maintaining our military advantage in multi-domain operations, given that adversaries have developed tactics and techniques to degrade, deny, and spoof our C3 systems.

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

I understand that the Department is addressing investment shortfalls as part of its digital modernization efforts, and I believe that DoD must ensure it continues to prioritize the C3 capabilities and resiliency needed for high-end conflict.

What is your assessment of the effectiveness of the Council on Oversight of the National Leadership Command, Control, and Communications System (NLC3S) as authorized under section 1052(f)(3) of the FY 2014 NDAA? How can the Council's effectiveness be improved?

The DoD CIO is a member and secretariat of the NLC3S co-chaired by the Vice Chairman of the Joint Chiefs of Staff and the USD(A&S). I believe the Council has been effective in ensuring that National Leadership Command Capability (NLCC) is able to meet the needs of the President and other senior leaders and raising critical issues to the

Department's senior leadership. If confirmed, I will review how the effectiveness of how the Council might be improved.

There has been much discussion about the importance of networking and connecting warfighting capabilities across air, land, and sea platforms through the Joint All-Domain Command and Control (JADC2) initiative.

What is the role of the CIO in developing and implementing solutions to JADC2 objectives?

The DoD CIO has been an integral member of the JADC2 effort and CFT since its inception. DoD CIO has collaborated with Department stakeholders on the conceptual design and development of the JADC2 Strategy and Implementation Plan, but the main DoD CIO role is as an enabler. Each JADC2 initiative relies on existing DoD CIO-led IT modernization efforts for success, such as JWCC, cybersecurity based on Zero Trust, and transport resiliency.

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

Tactical data links (TDLs) are foundational to the command and control (C2) of the Joint Force, our allies, and coalition partners. It is my understanding that the Department has three lines of effort to ensure that airborne data links are resilient: (1) advocating that Services expeditiously close identified gaps by rapidly fielding the Multifunctional Information Distribution System (MIDS) Program of Record for Link 16, (2) identifying legacy TDLs that are vulnerable or require replacement, and (3) accelerating the implementation of advanced capabilities to increase the resiliency, robustness, and capacity of tactical networks.

If confirmed, specifically what would you do to facilitate development and implementation of JADC2 concepts?

If confirmed, I would leverage the DoD CIO statutory authorities to use the Budget Certification process, to include providing annual Capability Planning Guidance, to ensure the successful implementation of the JADC2 Strategy, ensuring the optimal delivery of capabilities to the Joint Forces. In addition, I would continue to drive JADC2 enablers including access to cloud compute and storage; resilient transport; and robust cybersecurity.

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, from the CIO's role with regard to infrastructure and networks that traditionally would be regarded as administrative or otherwise non-warfighting in nature? Does the CIO's authority extend to warfighting networks and systems in the Department? Is the CIO qualified and resourced to serve as the official with a fundamental role in the warfighting infrastructure of the Department?

In my view, networks are converging as we start focusing on data-centric architectures. Business and warfighting infrastructure are leveraging and implementing the same technologies and formats at the network transport, compute/store and cybersecurity layers, with the primary difference at the tactical edge in providing increased survivability. I believe the DoD CIO is sufficiently resourced to drive the modernization of warfighting infrastructure across the Department.

Please describe your view of the CIO's role with respect to overseeing the cryptographic accounts at the National Security Agency and recent efforts to build new facilities or upgrade existing facilities and infrastructure at the NSA for cryptographic key and management infrastructure across the DOD?

DoD CIO is the PSA responsible for DoD cybersecurity and protection of NSS. In this capacity, DoD CIO collaborates with NSA, as the NSS National Manager, to modernize the key management infrastructure across DoD. NSA's tenets call for a Key Management Enterprise (KME) that permits a "person-out-of-the-loop" electronic crypto key distribution from the generation of the key through the key processor to the End Crypto Unit (ECU). Additionally, they require an inventory of cryptographic devices that are more robust, modular, scalable, capable, net-centric, and durable. These tenets enable more effective and efficient performance including reduced inventory, expanded data rates, simplified upgrades, lower life cycle costs, and ensured global information grid-compatibility in addition to eliminating current key vulnerabilities. Modernization of the KME is required to ensure cryptographic keying material and supporting data is protected at the highest level throughout the enterprise.

How should these same efforts be applied to the development and distribution of nuclear command and control products, in your view?

I believe that modernization of nuclear command and control products is critical to ensure the highest levels of security. The same tool sets used to upgrade cryptographic key and management infrastructure should be used to modernize nuclear command and control products across the DoD. However, it must remain a separate and isolated activity from the overall enterprise modernization processes given its sensitivity.

Information Technology Workforce and the Cyber Excepted Service

The Chief Information Officer serves as the functional community manager for 18 civilian occupational specialties, accounting 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. The CIO's diligent performance of these functions is critically important to the Department's ability to evolve 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, what factors would you

apply to a determination as to whether a certain position should be filled by military, civilian, or contractor personnel?

I believe that USD(P&R) has established an effective policy and structure for the determination of workforce mix across the Department. This policy dictates that risk mitigation be given precedent over cost savings or other efficiencies. The ability to continually evaluate these decisions based on risk as the domain evolves is crucial to the Department's agility in this domain. To enhance and complement the USD(P&R) process of workforce determination, the Defense Cyber Workforce Framework and the DoD 8140 policy series provide a management framework and governance structure for the cyberspace workforce that can be leveraged to manage military, civilian, and those contracted to augment the force.

What is your view of the appropriate mix between the uniformed cyber workforce and civilian employees?

I believe the current mix is appropriate. Current projections have this mix at approximately 45 percent military, 30 percent civilian, and 25 percent contractor across the full spectrum of the DoD cyber workforce. Overall, the current mix brings diversity of thought and experience, which I view as a strength of the Department.

Each Military Department and DOD Component is competing for the same set of skilled and experienced employees—those 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 Cyber Workforce Management Board provides the tools to successfully recruit, retain and develop members of the cyber workforce. The DoD Cyber Workforce Framework provides a more detailed focus than traditional civilian occupational series, and, based on its alignment with the National Initiative for Cybersecurity Education (NICE), it also provides a tool for Components to communicate with partners across government, industry and academia. In addition, it enables very targeted recruitment and retention by location and specialty. The largest percentage of the DoD cyber workforce are military members, who are developed through established training pipelines, including best practice programs for some operational roles.

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?

In my view, I believe most, if not all, of the DoD civilian cyber workforce should be eligible for Cyber Excepted Service (CES). Expanded eligibility would maximize the benefits of the enhanced recruitment, retention, and development flexibilities authorized under CES.

In your view, how effective is the Cyber Excepted Service Workforce in meeting the requirements for a highly qualified and competent cyber workforce?

In my view, the Cyber Excepted Service is highly effective in meeting the requirements for a qualified and competent workforce. Further, effectiveness will continue to grow as the number of organizations leveraging CES is expanded. Even so, competition for this workforce is fierce and, if confirmed, training of the current workforce and enhanced recruitment and retention will be one of my priorities.

What actions would you take, if confirmed, to mitigate any gaps between cyber workforce capacity and capability?

If confirmed, I would continue the current path of the DoD Cyber Workforce Framework (DCWF), DoD 8140 policy series and CES utilization. The foundation of these efforts, supported in cooperation with partners in USD(P&R), USCYBERCOM, and the Military Departments, are providing significant benefits. As implementation activities continue, the analytics capabilities of the Advana business intelligence platform will be used to better analyze overall workforce numbers against readiness. I will also pursue re-skilling of our current workforce, and ensure publication of a new Cyber Workforce Strategy.

In your judgement, what additional authority does the Department needs to recruit and retain talent for the Cyber Excepted Service?

If confirmed, I will review the current authorities and make the appropriate recommendations to Congress.

Should management of the Cyber Excepted Service be transferred to the Under Secretary of Defense for Personnel and Readiness, in your view?

In my view, no. The DoD CIO works closely with USD(P&R) on program implementation. I understand that both organizations have agreed that the DoD CIO is the right functional lead for this area and, if confirmed, I will continue the strong partnership between CIO and USD(P&R).

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?

I understand that the DoD CIO currently tracks implementation metrics such as recruitment and retention data, combined with qualification and development information garnered from DoD 8140 policy implementation. I further understand that the DoD CIO is also developing and implementing an advanced analytics tool to enhance predictive analysis. As this capability continues to mature, I foresee this data being integrated with operational metrics such as readiness to provide a broader picture of force capabilities and gaps.

Command Climate Survey

In the context of your service as Principal Deputy CIO, did you administer 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?

No, I did not administer a command climate survey during my tenure as PDCIO.

If you have not administered such a survey, would you plan to do so, if confirmed? Please explain your answer.

Yes. In addition to encouraging my organization's participation in the annual Federal Employee Viewpoint Survey, if confirmed I would also work to develop and administer a DoD CIO-specific command climate survey at the earliest opportunity. I believe climate surveys are critical in identifying needs and concerns of the workforce, and help leaders identify areas that need improvement or adjustment to ensure an inclusive workplace environment that contributes to the organizational mission.

Sexual Harassment

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

What is your assessment of the current climate regarding sexual harassment, gender discrimination, and other harassment in the Office of the CIO?

I assess that the status on these areas is positive overall, but always meriting close supervision, as with any organization.

If confirmed, what actions would you take were you to receive or become aware of a complaint of sexual harassment, discrimination, or other harassment from an employee of the Office of the CIO, or an employee of an organization over which the CIO exercises authority, direction, and control?

If confirmed, I would act quickly and thoroughly to address any complaints of sexual harassment, discrimination, or other forms of harassment. I would ensure that the individual's chain of command is taking the complaint with the utmost seriousness, and will work closely with appropriate DoD authorities (Office of General Counsel, Washington Headquarters Service, etc.) to get advice and guidance. Additionally, I would ensure a positive, inclusive, and fair leadership climate, making clear that any sort of discriminatory or harassing behavior has no place in CIO or the DoD writ large.

Cyber Readiness Review

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 highlighted the urgent need for the Navy to modify its business and data hygiene processes to protect data as a resource.

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

In my view, the Department is keenly aware of the cyber readiness issues identified in the Navy review as well as those problem areas highlighted in other studies such as the Cyberspace Solarium Commission's report. As I understand it, the Department is now appropriately focused on the remediation and modernization efforts required to address these short-falls.

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?

In my view, shaping and molding an effective cybersecurity culture among DoD members is an institutional process that must occur across all Components, from the forward-deployed service member to the civilian at a CONUS installation. Over the past decade, I understand that DoD has moved away from the idea that cybersecurity is just a DoD CIO responsibility, but the responsibility of every DoD member. To improve this trend, I expect that DoD will continue to educate and hold its entire workforce responsible for the proper employment of cybersecurity practices in the performance of their jobs, and where practical, the use of technology to enforce proper cybersecurity practices. In September 2020, the Department initiated an effort to empower and hold key leaders accountable for improvements in DoD Cybersecurity through a revision of its cybersecurity policy for the deployment of a cyber-systems and applications. No longer is it just the system's operator, the component authorization official, or a program manager, but it is now the responsibility of all three to consult with each other to ensure any risks are appropriately mitigated. If confirmed, I would continue with this emphasis on ensuring that cybersecurity is a Department-wide responsibility, and not just for those in CIO or other IT organizations.

Relations with Congress

What are your views on the state of the relationship between the Office of the CIO and the Senate Armed Services Committee in particular and with Congress in general?

In my view, it is critical that the DoD CIO maintain close coordination and consultation

with Congress. If confirmed, I would commit to establishing and maintaining a close working relationship with the Members and their staffs.

If confirmed, what actions would you take to sustain a productive and mutually beneficial relationship between Congress and the Office of the CIO?

If confirmed, I commit to working collaboratively with Congress and Department of Defense oversight committees and responding to Congressional requests in a timely manner. This includes informing Members and their staffs of critical updates in a timely and transparent manner. I assure the Committee that I will serve as a partner with Congress.

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.

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

Yes.

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

Yes.

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

Yes.

Do you agree, without qualification, if confirmed, to keep this committee, its subcommittees, other appropriate committees of Congress, and their respective staffs apprised of new information that materially impacts the accuracy of testimony, briefings, reports, records—including documents and electronic communications, and other information you or your organization previously

provided? Please answer yes or no.

Yes.

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

Yes

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

Yes.

Do you agree, without qualification, if confirmed, to ensure that you and other members of your organization protect from retaliation any military member, federal employee, or contractor employee who testifies before, or communicates with this committee, its subcommittees, and any other appropriate committee of Congress? Please answer yes or no.

Yes.