Senate Armed Services Committee
Advance Policy Questions for Kirsten Davies
Nominee 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 to include overseeing and exercising authority, direction, and control over the Defense Information Systems Agency, cybersecurity activities, information technology systems, as well as matters related to spectrum and precision navigation and timing.

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

   The DoW CIO is the Principal Staff Assistant (PSA) and senior advisor to the Secretary of War on key areas such as Information Technology (IT) strategy, policy, management, and assurance, as well as cybersecurity, non-intelligence space systems, satellite communications, position, navigation and timing (PNT), spectrum, telecommunications, and the DoW information enterprise that supports DoW command and control (C2). The role focuses on advancing technology and cybersecurity to secure a competitive edge, fostering innovation through industry collaboration, promoting IT and cyber workforce development, and aligning departmental efforts to achieve modernization goals. The CIO reviews, recommends, and monitors IT and cybersecurity investments and budget requests across the Department to optimize resource use.

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

   If confirmed, I will work to ensure the Department's digital infrastructure supports the warfighter and remain open to any additional duties the Secretary assigns. I will approach all responsibilities with integrity, efficiency, and commitment to the mission.

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

   If confirmed, I would bring extensive private-sector experience in cybersecurity, IT leadership, and digital transformation, having served as Chief Information Security Officer at global organizations such as Unilever and The Estée Lauder Companies, Corporate Security Officer at Barclays Africa Group, and global Deputy Chief Information Security Officer at Hewlett Packard and Siemens. My expertise includes risk reducing and managing complex IT and Operational Technology (OT) ecosystems, driving innovation in emerging technologies like AI and automation, and aligning IT strategies with organizational goals. Additionally, my work as founder of the Institute for Cyber, advisor to key technology startups and venture capital groups, and as a member of the National Security Institute's Cyber and Tech Security Council has provided valuable insights into cyber and tech automation, risk management, and policy development, which I will leverage to support the Department's modernization priorities and goals.

4. **What is your understanding of the role the DOD CIO plays in oversight and management of the Defense Information Systems Agency?**

   The position of the DoW CIO has authority, direction, and control over the Director of the Defense Information Systems Agency (DISA). I understand the DoW CIO is responsible for providing strategic oversight and guidance to ensure DISA's operations align with the Department's mission priorities, including secure communications, network management, and cybersecurity. I would work to ensure DISA's capabilities effectively support warfighter needs and advance modernization efforts across the Department.

5. **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, I would prioritize setting a strategic path forward to support the next-generation technology and cybersecurity needs of our warfighters and national security. This would include continuing current initiatives such as advancing cloud computing capabilities to enhance scalability and resilience across the Department, accelerating the adoption of Zero Trust (ZT) principles across IT and Operational Technology (OT) to strengthen cybersecurity, prioritizing and accelerating the modernization of defense business systems to improve efficiency, integrating 5G technologies to support mission-critical communications, increasing focus on OT cybersecurity, and ensuring robust solutions for nuclear command and control, position, navigation, and timing systems. Transformation in policy, process, and technology would also be a priority, to build out the "rails" for AI and other innovations, supporting our warfighter, partner, and ally decision dominance. These efforts would align with the Department's strategic goals and ensure the information enterprise is prepared to meet evolving operational demands.

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

   The DoW CIO is responsible for developing and overseeing information security policies, as well as providing guidance on cybersecurity programs and architecture to safeguard the Department's digital infrastructure. The Principal Cyber Advisor, through the Assistant Secretary of War for Cyber Policy, focuses on oversight of military cyber operations and associated resources. If confirmed, I would work to ensure close collaboration between these roles to align cybersecurity policies with operational priorities and strengthen the Department's overall cyber posture.

7. **Do you believe this allocation of responsibilities should be changed or clarified? Please explain your answer.**

   If confirmed, I would focus on ensuring the current allocation of responsibilities is effectively implemented to support the Department's strategic goals. Collaboration and coordination between the DoW CIO and the Principal Cyber Advisor are essential to maintaining a strong cybersecurity posture and advancing operational priorities. I would work to identify any areas where alignment, clarity, or refinement could further enhance mission success.

Major Challenges and Opportunities

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

   One of the most significant challenges would be bolstering the security and ensuring the resilience of the Department of War Information Network (DODIN) against evolving threats from adversaries, including non-state actors. Additionally, addressing the growing need for a skilled cyber workforce to support the Department's mission-critical operations will be essential. I would focus on strengthening cybersecurity and resilience measures, enhancing workforce development, and preparing the Department for contingencies which, in turn, support warfighter readiness and safeguard national security.

9. **Describe significant opportunities to address these challenges that, in your view, DOD has been unable to leverage, or has only partially leveraged.**

   One significant opportunity for the Department is to enhance collaboration with private-sector cybersecurity experts and ethical hacker groups to identify and mitigate vulnerabilities in the Department's networks. Additionally, leveraging advanced threat-intelligence capabilities to better understand and counter state-sponsored hacker groups and cybercriminal organizations remains an area for growth. Another opportunity is reducing the barriers to entry for new, innovative technical and cyber capabilities to support agility and resiliency. If confirmed, I would focus on fostering partnerships and integrating innovative solutions to strengthen the Department's technology capabilities and cyber defenses, and address workforce development challenges.

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

If confirmed, I plan to establish clear frameworks for engaging private-sector cybersecurity experts and ethical hacker groups, ensuring their insights are integrated into the Department's security strategies. I will also drive the adoption of advanced technologies to enhance threat detection and response capabilities. Additionally, I will champion initiatives to expand and upskill the cyber workforce, ensuring the Department is equipped to address emerging threats effectively and without delay.

Civilian Control of the Military

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

If confirmed, I will ensure all decisions and actions as Chief Information Officer align with the principles of civilian oversight as outlined in the U.S. Constitution and federal law. I will prioritize collaboration with military leaders while maintaining clear accountability to the Secretary of War and other civilian authorities, ensuring that the Department's IT and cybersecurity strategies reflect civilian leadership and oversight at every level.

12. Based on your previous experience in industry, how would you integrate advice from the Office of the General Counsel into your decision-making processes, if confirmed, to ensure that legal, privacy and civil liberties considerations are incorporated into decision processes?

If confirmed, I will prioritize close collaboration with the Office of the General Counsel to ensure all decisions are fully informed by legal, privacy, and civil liberties considerations. Drawing from my industry experience, I understand the importance of integrating legal advice early in the decision-making process to mitigate risks and uphold compliance. This approach will ensure the Department's policies and initiatives are both effective and aligned with the law and Department policy.

Relationships with Other Department Offices

13. As Chief Information Officer for the Department, what do you perceive to be the appropriate relationship between you and the CIOs of the Military Services, the Joint Staff J6, and Defense Agencies?

If confirmed, I will foster a collaborative and coordinated relationship with the CIOs of the Military Services, the Joint Staff J6, and Defense agencies. My role will be to provide strategic, policy, and standards guidance, ensure a sound, secure, integrated and interoperable DoW IT architecture, collaborate to monitor and evaluate the performance of IT investments, ensure alignment with Department-wide priorities, and support their efforts to meet mission requirements while maintaining open communication and mutual accountability.

14. In your experience, what is needed to 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?

Consistency and unity of effort across the Department require clear, centralized guidance, sustained focus on and accountability for achieving outcomes to policies, programs and projects, combined with regular collaboration and communication among stakeholders. If confirmed, I will prioritize the development of shared goals, standardized frameworks, and governance processes to ensure alignment in strategy, planning, policy, and oversight.

15. In your experience, what do you believe is required to avoid unnecessary duplication between your efforts as the Department's CIO and the CIOs for each Military Service?

To avoid unnecessary duplication, it is essential to establish clear roles and responsibilities, along with mechanisms for regular coordination and information sharing. If confirmed, I will work to streamline processes, identify areas for consolidation, and ensure that efforts at all levels complement rather than overlap, maximizing efficiency and effectiveness across the Department.

16. If confirmed, what relationship would you build with USD(R&E) with respect to research, technology development, and prototyping activities to support current and next generation defense software, cybersecurity, information systems, spectrum, and networking capabilities?

If confirmed, I will build a strong partnership with USW(R&E) to align research, technology development, and prototyping efforts with the National Defense Strategy. Together, we will integrate availability, cybersecurity, and survivability requirements into capability designs, ensuring secure and resilient defense software, information systems, spectrum, and networking. This collaboration will accelerate the delivery of innovative solutions to the warfighter, addressing both current and future challenges.

17. If confirmed, what relationship would you build with USD(I&S) with respect to oversight and development of intelligence systems for the Department?

If confirmed, I would work closely with USW(I&S) as well as with the Intelligence Community (IC) to build information network and enterprise architectures, standards, and policies that support the IC-prioritized requirements for critical intelligence. Ensuring the USW(I&S) has a seat at the table in all DoW CIO governance bodies that oversee these supporting information technology systems, and their development, is the best way to achieve this.

18. **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?**

    If confirmed, my role will include establishing the strategic guardrails and enterprise services that enable secure software delivery across the Department. Through governance bodies like the Software Modernization Senior Steering Group, I will partner with USW(R&E) and USW(A&S) to ensure the complementary expertise of the Defense Digital Service is applied to our most critical challenges. This partnership, combined with insights from the U.S. Digital Service, will ensure a unified effort to provide superior digital capabilities to the warfighter.

19. **How do you view the relationship between the cyber operations elements to include the Commander of United States Cyber Command? What actions would you take, if confirmed, to ensure effective collaboration on building and security networks as well as developing the cyber workforce?**

    If confirmed, I will prioritize collaboration with USCYBERCOM to ensure effective integration of cybersecurity policy, network operations, and cyber missions. I will focus on advancing joint efforts like the cyber campaign plan, enhancing real-time monitoring of the Department of War Information Network (DODIN) and supporting the development and training of the Cybersecurity Service Provider workforce to address evolving challenges and opportunities.

20. **In confirmed, what would your relationship be with the Assistant Secretary of Defense for Cyber Policy? What actions would you take to ensure that there is alignment of policy for cyberspace operations and cyber support across the cyber operations forces?**

    If confirmed, I will work with ASW-Cyber Policy to integrate offensive cyber activities with cybersecurity activities, as appropriate, to enable the Department to take holistic and coordinated efforts in addressing cyber threats that face the Department and the nation.

Budget Review and Standards-Setting Authority

Section 909 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2018 empowered the DOD Chief Information Officer to exercise budget review and certification authority to ensure that the budgets of Department of Defense components with responsibilities associated with any activity specified in section 142(b)(1) of title 10, U. S. Code, are adequate for such activities.

21. **If confirmed, how will you use this budget review and certification authority to shape the modernization and prioritization of cybersecurity and information technology infrastructure?**

If confirmed, I will explore ways to ensure the DoW CIO's budget certification authority drives risk-informed IT modernization, cybersecurity and related investments. I will be looking to prioritize investments that improve the Department's cybersecurity and resilience posture while modernizing our IT and communications infrastructure. This would include prioritizing initiatives that streamline operations, reduce redundancy, demonstrably improve security posture, and advance the Department's warfighting capabilities.

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

    If confirmed, I will ensure directives, policies, and standards are clear, actionable, and aligned with the Department's mission priorities, while engaging stakeholders early to build consensus and address potential challenges. I will establish regular reporting mechanisms, conduct compliance reviews, and leverage performance metrics to assess adherence across Components. Additionally, I will maintain open communication channels to provide guidance and address any obstacles to consistent and timely implementation.

23. **In your view, how should decisions regarding the technology debt of DOD software and IT systems be incorporated into budget certification processes to help drive modernization across the Department and the military services?**

    If confirmed, I would work with leadership in the DoW Components to ensure transparent accounting of current technical debt and would assess ways that we could tie the DoW CIO's budget certification authority to credible plans for technology debt reduction. This would include requiring Components to adequately resource programs and projects that improve and modernize our IT capabilities and cybersecurity posture. It is important that the Department incentivize efficient modernization and decommissioning of legacy systems with clear metrics and accountability.

National Defense Strategy

On May 1, 2025, the Secretary of Defense initiated the development of a new National Defense Strategy (NDS) centered around the imperative of peace through strength.

24. **Technology is likely to play a central role in the new NDS, specifically software-defined technology that enables agile development and fielding. This agility must also be balanced by security. If confirmed, what actions will you take to support the development of an NDS that strikes this balance?**

If confirmed, I will promote the approach that comprehensively incorporates refinements across people (skills), processes, and technology. For example, I will ensure the appropriate training for and adoption of modern practices that leverage agile delivery approaches. I will ensure reuse of proven enterprise capabilities for accelerated and secure deployment of software into weapons systems. Through policy, I would establish a balance between fast and secure, identifying the requirements and standards needed to protect software throughout its lifecycle (e.g., Risk Management Framework, supply chain risk management, reciprocity) and integrating those with delivery through modern software development practices (e.g., DevSecOps, software factories) and technologies (e.g., dynamic and static code scanning, software gate management).

Acquisition of Information Technology

NDAAs since 2009 have enacted sweeping reforms of defense acquisition organizational structures, processes, and systems, which include emphasizing shortening acquisition cycle times, diversifying options for acquisition approaches and mechanisms, and delegating acquisition authorities. More recent reforms have focused on revising and simplifying complex compliance structures to promote employment of the "agile" development of software-intensive systems, applying methods to deliver continuous product improvement, at greater speeds.

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

Data and data science are fundamental to a successful acquisition reform and agile development, serving as a feedback engine that drives measurable, transparent, and adaptive processes. If confirmed, I will champion a data-driven approach using performance metrics and user feedback to provide the empirical evidence needed to justify acquisition reforms and ensure agile teams deliver continuous value to the warfighter, replacing subjectivity with objective insights to accelerate the delivery of superior capabilities.

26. Secretary Hegseth's March 6, 2025, memorandum "Directing Modern Software Acquisition to Maximize Lethality" mandates the SWP as the preferred acquisition method for all software development components. If confirmed, how will you address the cultural shift required within the acquisition workforce to successfully implement Agile software development practices across DOD programs, particularly in weapon systems that have traditionally followed waterfall methodologies?

Making the Secretary's' mandate a reality depends on fundamentally changing our culture for acquisition professionals and system integrators. If confirmed, I will build upon the CIO's Workforce Strategy, working in partnership with USW(A&S) to focus these initiatives on driving modern practices and technologies. Our joint efforts will provide tailored agile training, modern tools, and updated incentives to empower our professionals, move beyond legacy waterfall processes, and deliver capabilities quickly. I'll partner with USW(A&S) and the Director of the Software Cadre to support the Secretary's memo "Directing Modern Software Acquisition to Maximize Lethality" to address needed reforms.

27. What specific metrics will you establish, if confirmed, to measure the effectiveness of the SWP implementation across DOD?

While responsibility for the Software Pathway rests with the USW(A&S), the CIO plays a crucial role in ensuring the supporting infrastructure and policy are effective. If confirmed, I will focus on metrics that assess the value provided to the DoW including speed of delivery to warfighters, security of solutions developed and delivered, and "fail fast/fail forward" methodology adoption. Software factories are an important part of delivering capability, and I will ensure the adoption of secure DevSecOps pipelines and reduction of known vulnerabilities in deployed systems. These measures will help ensure that SWP implementation is improving both the pace and the security of software delivery across the Department.

28. If confirmed, how will you lead by example by using these reforms and methods in your own acquisition efforts—including market research, testing and certification, and contracting vehicles—to leverage non-traditional cybersecurity and information technology performers and solutions?

If confirmed, I will lead by example by prioritizing clear communication with industry to ensure they understand the Department's unique requirements for reliability, cybersecurity, and operational capabilities. I will leverage innovative contracting vehicles, test and learn processes and sandbox evaluations, rigorous evaluation criteria, and collaboration with organizations like the Defense Innovation Unit to integrate cutting-edge solutions from non-traditional performers, ensuring the Department acquires the best technologies to support its mission effectively.

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

Both approaches have a role to play. If confirmed, I would continue to emphasize making commercial solutions the presumptive first choice, provided they meet mission, security, and sustainability thresholds. I would also propose to develop/retain government-unique solutions only where commercial offerings cannot satisfy truly unique mission needs. Decision-making should be based on key criteria like mission criticality, security and supply-chain risk, technology pace, lifecycle costs, and interoperability and enterprise standards.

30. What are the pros and cons in your view of a procurement approach of information technology-as-a-service? Are there use cases where you think this makes less sense for DOD to pursue? What is required to change in the acquisition processes to ensure this approach proves effective and efficient?

Information technology-as-a-service has the potential to provide greater security and resiliency partnered with faster access to innovation, scalability, flexibility, and predictable costs and allows components in the Department to focus on core missions. This can be seen in as-a-service use to support commodity and enterprise services (e.g., cloud hosting, identity management, collaboration, helpdesk, network transport). The Department should continue to use tools outside of as-a-service to meet mission needs. If confirmed, I will work with the USW(A&S) to update these acquisition processes that enforce security and interoperability standards and maintain in-house technical expertise so that outsourcing strengthens mission assurance.

31. 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 should lead in delivering enterprise IT and cybersecurity solutions, focusing on innovation, integration, and cost-effectiveness. If confirmed, I would work with DISA to address challenges, streamline acquisition, and ensure resilient capabilities that meet the Department's evolving needs.

32. How could DISA improve its performance in this regard in your view, including technology development and systems acquisition? If confirmed, what steps would you take next, and why?

DISA should prioritize faster, outcome-focused acquisitions using open architectures and modern development practices like DevSecOps. If confirmed, I would ensure alignment with mission needs, enforce open standards, and hold vendors accountable for delivering secure, resilient capabilities that enhance readiness and adaptability.

33. In your view, what role should the National Security Agency's Cybersecurity Directorate play in facilitating cybersecurity market research, industry engagement, testing, and acquisition across the Department of Defense? If confirmed, what "next steps" would you take to move this initiative forward, and why?

The National Security Agency's Cybersecurity Directorate plays a vital role in supporting the Department of War by providing intelligence, technical expertise, and threat information to enhance cybersecurity market research, industry engagement, testing, and acquisition. If confirmed, I will work to strengthen collaboration with NSA across DoW to integrate threat intelligence into market research, improve access to cybersecurity insights for decision-makers, and increase the use of red-team testing and supply chain risk assessments as part of acquisition processes. This approach will address vulnerabilities, enhance readiness, and ensure the Department remains resilient against evolving threats.

34. **What is your opinion on the use of software bills of material in DOD contracts to gain better insight and oversight for the provenance of the software being incorporated into DOD systems? Are there ways to couple this with other software assurance techniques in order to improve the security and reliability of software-intensive systems? Are there best practices from industry that you think DOD should be adopting that you do not believe they are using now?**

    Software bills of material (SBOMs) are an important tool for managing software supply chain risk, but they are not sufficient on their own. If confirmed, I will ensure the Department not only collects SBOMs in contracts but also develops the people, processes, and tools needed to analyze them and act on the results. SBOMs should be integrated with other assurance practices, such as secure development, automated code scanning, and continuous monitoring so the Department can reduce risk and improve reliability in software-intensive systems.

Cybersecurity Architecture

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

    The Department's major cybersecurity challenges include managing the complexity of its networks, aligning the various capability operations and ownerships, integrating new technologies with legacy systems, addressing resource constraints, and keeping pace with evolving threats. If confirmed, I will focus on identifying gaps and overlaps to streamline efficiencies and defenses, modernizing systems and capabilities, enhancing threat detection, and investing in cyber talent to strengthen the Department's cybersecurity posture.

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

    The Department's cybersecurity programs and capabilities face challenges in detecting and defeating advanced persistent threats due to the complexity of its networks. If confirmed, I will prioritize building seamless collaboration and capabilities across cyber defenses; advancing Zero z-trust implementation; enhancing Cybersecurity Service Provider capabilities; and leveraging AI, automation, and proactive threat hunting to strengthen defenses and stay ahead of adversaries. Continuous improvement and collaboration will be key to addressing these evolving threats.

37. What programs, capabilities, or common infrastructure should the Department of Defense prioritize for modernization to improve its cybersecurity posture and resiliency in the face of advanced persistent threats? If confirmed, how would you address the gaps between DOD's legacy systems and the Department's objective programs, capabilities, and infrastructure?

If confirmed, I would prioritize modernizing the Department's cybersecurity posture by improving end-to-end visibility and operations; advancing data-centric protections; leveraging AI and analytics; and enhancing identity, device, session, and data trust. Addressing gaps in legacy systems requires a dual approach: implementing compensating controls for immediate resilience while securing funding and setting timely, measurable milestones to modernize critical systems. Collaboration and updated policies will be essential to align efforts with the operational fight ahead.

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

The Department's cybersecurity operators and service providers are highly skilled and effective, but they must continuously evolve to address emerging threats. If confirmed, I would focus on enhancing their real-time visibility and detection capabilities by improving network, endpoint, cloud, and software inventory; leveraging advanced analytics (e.g., user and entity behaviors); integrating advanced technologies and constant innovation, and enriching data to ensure they are prepared for tomorrow's fight.

39. The Joint Forces Headquarters-Department of Defense Information Networks (JFHQ-DODIN) and DISA play critical roles in ensuring security and defense of the DOD information networks. If confirmed, how will you ensure these organizations are sufficiently resourced, manned, and equipped to serve as operational command and control hubs for the Department of Defense's cybersecurity efforts?

If confirmed, exercising my responsibility to certify the Cybersecurity and IT Budget, I will ensure that resources for DISA and JFHQ-DODIN are on my priority list and their requirements are included in the DoW CIO Capability Programming Guidance (CPG). I will leverage the Program Objective Memorandum cycle and prioritize issue papers that resource DISA and JFHQ-DODIN activities. I will also work with other DoW components to ensure the DoW Cyber Defense Command (formerly JFHQ-DODIN) is sufficiently resourced, manned, and equipped through the Cyberspace Operations Budget.

40. In April, the acting Chief Information Officer announced the Software Fast Track program that looked to streamline current Risk Management Framework requirements to support more rapid Authority to Operate approvals. If confirmed, what steps will you take to continue these efforts and ensure more rapid delivery of critical software-first systems?

If confirmed, I will build on the Software Fast Track initiative by promoting automation, standardized templates, interoperability, and continuous integration to accelerate Authority to Operate decisions. I will also prioritize collaboration across the Department to reuse security assessments and streamline procurement paths, ensuring faster delivery of secure, mission-critical software to the warfighter.

41. In your view, how could the Department be working to make the Cybersecurity Maturity Model Certification (CMMC) 2.0 process both more effective, and more user friendly for the many industry providers that will now need to meet these requirements?

If confirmed, I will work to make the CMMC 2.0 process more effective and user-friendly by implementing an approach that balances strong cybersecurity protections with minimizing industry burden, especially for small businesses, and advancing innovation for the Department. I will prioritize communication with businesses, collaboration with stakeholders to ensure accountability and compliance, tailoring of approach based on risk, and building security and resilience into the Defense Industrial Base.

42. If confirmed, how would you propose working with the DOD Office of Small Business Programs to provide tools and support for small businesses to navigate the cybersecurity environment in DOD?

If confirmed, I will strengthen the partnership between the DoW CIO and the Office of Small Business Programs to enhance initiatives like Project Spectrum, APEX Accelerators, and the Manufacturing Extension Partnership. These efforts will focus on improving cybersecurity education, streamlining compliance, and providing affordable solutions to help small businesses meet requirements while supporting the resilience of the Defense Industrial Base.

<u>Information Technology, Networking, and Cloud</u>

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

The Department is facing the challenges that come with modernizing an information technology enterprise of this scale. The need to modernize networks, Defense Business Systems, and command and control infrastructure is made more difficult because of the scale of the Department and legacy processes that can slow down innovation. If confirmed, I will work across the Department to improve processes and overhaul how we address our modernization activities. The Department can do this by prioritizing key areas for IT and cloud advancement, while risk reducing legacy systems. Additionally, we must continue to strengthen our cybersecurity through Zero Trust architecture, robust data protection, and secure information sharing.

44. If confirmed, what management actions, policies, acquisition efforts, and timelines would you see as most critical to address the challenges or deficiencies in the areas of networking, commercial technology adoption, and utilization of cloud computing?

If confirmed, I will drive consistent management actions by accelerating Zero Trust implementation and improving transparency on cloud spending so Congress can see where taxpayer dollars are going. Second, I will work to ensure our policies keep pace with mission needs, including updating cloud security guidance and making certain we can share appropriate data securely with allies and partners while simultaneously protecting that data from our adversaries. Third, I will support acquisition efforts that streamline access to commercial cloud through Joint Warfighting Cloud Capability (JWCC), leveraging Other Transaction Authority and partnerships with the Defense Innovation Unit, and avoid duplicative contracting that wastes resources. Finally, I will push for faster timelines by moving away from lengthy, multi-year authorizations and migrations and toward incremental adoption that delivers capabilities to the warfighter sooner.

45. DOD and the services have invested significantly in developing enterprise contracts, specifically in cloud computing services under the Joint Warfighting Cloud Capability (JWCC) contract, to support the Department. Yet, the use of these contracts is inconsistent. If confirmed, how will you use lessons learned to posture any follow-on contracts to provide greater success?

JWCC is a critical enterprise tool for accessing commercial clouds at scale, but its success depends on clear requirements, strong governance, and accountability for user adoption. If confirmed, I will collaborate across the component CIOs to drive user adoption, and ensure follow-on contracts emphasize flexibility, reduce duplicative efforts, and align with the Department's broader modernization strategy. I will also prioritize vendor incentives tied to cost savings, security, faster software delivery, and user satisfaction to deliver the best outcomes for the warfighter.

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

If confirmed, I will measure cloud migration in three ways. First, by adoption, looking at whether programs are moving workloads to JWCC and doing so quickly and securely. Second, by performance, tracking cost efficiency, reliability, and scalability to provide transparency into the value which cloud delivers over legacy systems. And third, by mission outcomes, ensuring cloud enables faster software delivery, stronger cybersecurity, and better decision-making with real-time data. These measures together will be assessed for true warfighter advantage, resilience, security, optimization, and cost efficiencies.

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

If confirmed, I will work to make data discoverable by driving common data standards and governance so that information can be found and used appropriately across the Department. I will also drive the use of analytics and business tools already available through Department commercial cloud contracts, while providing the training and support needed to help the workforce adopt them effectively. I will further leverage these same business tools and analytics, and others, to assure usage and drive accountability. And finally, I will strengthen networking and cybersecurity performance by advancing Zero Trust, expanding continuous monitoring and authorization, and prioritizing modernization so that the Department can take full advantage of cloud services with confidence in their security and reliability.

48. International collaboration has become increasingly important for DOD activities and operations. If confirmed, how will you work across the services and through DISA to ensure warfighters and the combatant commands have mission partner environments that can securely facilitate operations with key allies and partners?

If confirmed, I will work across the Military Services to ensure that mission partner environments are designed with common standards, so they are interoperable from the start, rather than built as isolated solutions. Second, I would collaborate closely with the Director of DISA to strengthen the governance, infrastructure and cybersecurity that underpin these environments, making certain they can operate at multiple classification levels while still protecting sensitive U.S. and allied data. Third, I would make sure these environments are aligned to operational requirements, with input from the combatant commands to guarantee that they are truly usable at the speed of operations.

49. In light of GSA's recent directives regarding IT contract reviews and consolidation, what will be your strategy, if confirmed, for reviewing legacy IT contracts that may not align with the Secretary's software acquisition guidance, and how will you prioritize which contracts to modify, terminate, or allow to continue?

If confirmed, I would look to prioritize eliminating duplicate legacy contracts and then move towards consolidating medium-risk contracts into enterprise vehicles while protecting and scaling those that already align with DoW software acquisition guidance. This could be done by implementing commercial best practices like adopting “review once, use many times”; mandating enterprise contract clauses requiring zero-trust compliance, SBOMs, etc.; leveraging category management by IT commodity, and engaging with mission owners early on to avoid resistance.

50. **Section 1546 of the FY25 NDAA requires the Department to develop a risk framework for foreign mobile applications of concern to help address gaps that have allowed applications like TikTok to find their way onto DOD issued mobile devices. Based on your experience in industry, how would you recommend DOD approach getting its arms around this challenge?**

    If confirmed, I will ensure that the Department aggressively reviews its application vetting processes and adopts innovative ways to stay ahead of the threat. We must ensure strong collaboration amongst the DoW's cybersecurity experts and industry partners to ensure we have controls, policies and systems in place to protect the Department’s data in case undesired applications somehow find their way onto DoW issued devices. Further, the Department should establish a multidisciplinary authoritative team of experts to continuously evaluate the mobile threat landscape, along with enhancing awareness and training to ensure end users are always informed. Finally, the Department should use technologies that block and remove undesired and/or unauthorized apps from devices.

<u>**Zero Trust**</u>

In April 2025, Randy Resnick, director of the DOD's Zero Trust Portfolio Management Office, highlighted specific timelines for achieving Zero Trust across different domains: IT systems by 2027, Operational Technology by 2030, and Weapons Systems by 2035. These timelines, particularly for Operational Technology and Weapons Systems have many members concerned in light of the threats from Chinese persistent cyber threats such as Volt and Salt Typhoon.

51. **The 2027 timeline for implementing Zero Trust across DOD IT systems is rapidly approaching. What do you see as the most significant challenges to meet this deadline, and, if confirmed, what steps would you take to ensure the appropriate investment or policy changes are prioritized to address these challenges?**

    The most significant challenges to meeting the 2027 Zero Trust deadline include policy misalignment, accountability for implementation, data interoperability, and resource prioritization. If confirmed, I will prioritize a review of the Zero Trust plan and ensure focused efforts to updating policies and assurance which drive Zero Trust implementation, accountability metrics for implementation, accelerating efforts to enhance data sharing and interoperability to ensure the Department meets its goals on time, and assessing and making recommendations for resource prioritization.

52. **Given the 2030 timeline for implementing Zero Trust for Operational Technology systems, if confirmed, how will you approach the unique security challenges of OT environments that differ substantially from traditional IT networks?**

    If confirmed, I will address the unique security and operational challenges of Operational Technology (OT) environments by leveraging a flexible, risk-based approach that accounts for hybrid IT/OT systems and legacy infrastructure. I will prioritize collaboration with OT experts and industry to implement tailored Zero trust solutions and processes that achieve security outcomes while respecting operational constraints. Compensating controls will also be pursued as a potential solution, especially to implement more rapid security protocols in constrained environments.

53. **What is your assessment of the current state of Zero Trust implementation across DOD, and how would you address any disparities, if confirmed, in progress between different components?**

    The Department is making steady progress toward achieving Target Level Zero Trust by FY27. If confirmed, I will address disparities by closely monitoring progress, driving accountability for the adoption, and advocating for prioritization of resources to ensure implementation across the Department.

54. **The DOD announced plans to release Zero Trust guidance for Operational Technology by summer 2025. What input would you want to provide, if confirmed, to this guidance, and how would you ensure it properly addresses the security needs of critical infrastructure within DOD?**

    If confirmed, I will ensure the Zero Trust guidance for Operational Technology addresses the unique security needs of critical infrastructure by emphasizing tailored, risk-based approaches that align with operational constraints. I will also prioritize collaboration with stakeholders to support diverse vendor implementations while maintaining consistent Zero Trust principles.

Critical Infrastructure

The 2023 Military Cyber Strategy and testimony from multiple administration witnesses affirm that the PRC will be positioned to be able to attack U.S. critical infrastructure (CI) in connection with preparations for, and the execution of, military operations. The aims of such attacks will be to inhibit the mobilization, deployment, and sustainment of U.S. forces and to sow chaos in the United States. The publicly announced detection of the campaign conducted by the PRC Volt Typhoon cyber actor provides credible confirmation of these forecasts.

55. **What do you view as the appropriate role for the DOD Chief Information Officer in securing the defense industrial base and national security innovation**

base from adversary cyber threats to ensure the integrity and security of DOD's classified information, controlled unclassified information, and key data?

The DoW Chief Information Officer plays a critical role in securing the Defense Industrial Base by fostering collaboration, enhancing threat intelligence sharing, and driving the adoption of rigorous cybersecurity standards. If confirmed, I will prioritize proactive defense measures, insider threat detection, and supply chain risk management to protect critical defense data from adversary cyber threats.

56. If confirmed, what "next steps" would you take to support activities protecting defense critical infrastructure?

If confirmed, I will prioritize integrating cybersecurity and mission assurance efforts to protect defense critical infrastructure by institutionalizing mission-relevant terrain-cyber (MRT-C) analysis. This would provide Combatant Commanders with near real-time insights into cyber risks and dependencies, ensuring the availability and security of critical assets during operations.

57. What do you view as the appropriate role of the DOD CIO with respect to securing National Security Systems across the government? What actions will you take, if confirmed, to mitigate system vulnerabilities, and to what effect? If confirmed, what next steps would you take to move this initiative forward, and why?

The DoW CIO plays a critical role in securing National Security Systems by establishing policy and standards and ensuring their implementation across the federal government. If confirmed, I will collaborate with Committee on National Security Systems (CNSS) and Department stakeholders to highlight and address vulnerabilities, enforce accountability, and ensure these systems are resilient against evolving cyber threats.

58. 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? If confirmed, what "next steps" would you take to move this initiative forward, and why?

If confirmed, I will ensure the DoW CIO drives adoption of secure development practices across the Department, including automated code scanning, continuous testing, and rigorous supply chain risk management. I will also promote shared standards and training to help developers build security into every stage of the software lifecycle. As next steps, I would prioritize integrating these practices into acquisition and DevSecOps pipelines to reduce vulnerabilities and deliver trusted capabilities faster.

Data Management and Business Systems

Section 910 of the NDAA for FY 2018 transferred responsibilities for data and business system research and development, acquisition, and management to various offices across the Department of Defense.

59. **What is your understanding of the respective responsibilities of the Under Secretary of Defense for Acquisition and Sustainment (USW(A&S)) and the Chief Information Officer for the acquisition of cybersecurity, information technology, and command, control, and communications systems, including contracting and software development?**

    The USW(A&S) is responsible for the acquisition system, including contracting authority and management of the Software Acquisition Pathway. The DoW CIO sets policy and standards for cybersecurity, information technology, and command, control, and communications, and ensures that systems are interoperable, secure, and aligned with enterprise architectures. If confirmed, I will work closely with the USW(A&S) to ensure our roles are complementary and that acquisition programs benefit from both strong technical standards and effective acquisition execution.

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

    If confirmed, I will work closely with the USW(A&S) to ensure our responsibilities are clearly defined and aligned to support the warfighter effectively. While the current allocation of responsibilities provides a strong foundation, there may be opportunities to clarify roles further to reduce overlap and improve efficiency. I will prioritize collaboration and communication to address any challenges and ensure our efforts are fully coordinated toward achieving mission success.

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

The USW(R&E) focuses on driving technology and rapidly maturing artificial intelligence (AI) capabilities into prototypes for transition. The USW(A&S) ensures that AI moves from prototype to programs of record effectively, with secure, maintainable, and affordable lifecycle management. Additionally, the CIO partners with the Defense Innovation Unit (DIU) to accelerate the adoption of commercial AI capabilities for specific operational needs. The DOW CIO drives the policy, standards and architecture (implemented by component CIOs), which ensures the secure digital foundation for data, networks, could and cybersecurity so that AI systems can operate reliably. Further, the DOW CIO assures all of the same, providing governance and accountability.

.

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

This allocation of responsibilities provides a solid foundation, but AI's unique nature as an evolving capability requires close collaboration across innovation, acquisition, IT, data, cybersecurity, and operational domains. If confirmed, I will focus on strengthening partnerships to ensure AI is integrated seamlessly across its full lifecycle, from lab to the battlefield use, and will further collaborate to have continuous review of responsibilities to ensure the Department is dynamic and future fit for innovation needs.

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

The USW(R&E) focuses on science, technology, and prototyping; the USW(A&S) oversees transition and fielding; and the DoW CIO ensures enterprise IT, cybersecurity, and interoperability standards to scale new capabilities. If confirmed, I will align CIO policies and services with USW(R&E) priorities and USW(A&S) pathways to integrate, secure, and scale emerging technologies like AI/ML, zero-trust identity, and cloud-native computing. I will also prioritize modern software practices like DevSecOps and automated risk management to improve speed, security, and reliability across the Department's information enterprise.

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

The Electromagnetic Spectrum Operations EXCOM provides senior oversight and coordination on electromagnetic warfare matters, while the CIO, as the designated senior official, is responsible for implementing the Department's Electromagnetic Spectrum Superiority Strategy and overseeing related policies. If confirmed, I will ensure alignment between these roles to advance spectrum superiority and support mission success.

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

If confirmed, I look forward to receiving a briefing on current activities and coordinating across the Department to consider if any changes or clarifications are required to ensure roles, responsibilities, and accountability are clear to best support lethality and the warfighter.

Electromagnetic Spectrum Policy and Operations

Spectrum remains a highly strategic resource for both commercial and defense uses. As a result, the Department has been tasked to support and participate in multiple studies on their requirements for portions of the spectrum for national security operations. In 2024, the CIO re-launched Partnering to Advance Trusted and Holistic Spectrum Solutions (PATHSS) under the National Spectrum Consortium (NSC). DOD has also invested significantly in spectrum sharing technology, which many believe are critical to future spectrum operations.

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

Given the electromagnetic spectrum is a limited natural resource, there are competing demands on the economic and security needs for spectrum use to meet the goals of this Administration. As the nominee, I understand that adversary actions, commercial development, and regulatory constraints impact U.S. forces' freedom of action in the spectrum. Ensuring such freedom of action will require new ways of thinking about access, sharing, and maneuvering in the spectrum. Our adversaries have recognized the U.S. military's reliance on spectrum-dependent capabilities and are seeking to exploit this vulnerability.

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

U.S. adversaries, such as China, have invested heavily over the course of decades in spectrum concepts and capabilities designed to undermine U.S. military superiority. If confirmed, I look forward to receiving a classified briefing on the capabilities and will work across the Department to set the conditions for advanced capabilities and increased lethality.

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

If confirmed, I will support short-term efforts to advance spectrum sharing capabilities, such as Advanced Spectrum Coexistence and Dynamic Spectrum Sharing, to balance commercial needs with warfighter capabilities. In the long term, I will prioritize modernizing spectrum IT infrastructure with cloud-based solutions to enhance resiliency, scalability, and operational effectiveness.

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

If confirmed, I believe spectrum sharing is a practical approach to increasing commercial spectrum access while ensuring the warfighter retains the necessary spectrum for homeland defense and national security. While challenges exist, opportunities like Advanced Spectrum Coexistence (ASC) and Dynamic Spectrum Sharing (DSS) offer actionable solutions to balance these priorities effectively.

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

If confirmed, I will assess the current structure, receive classified threat briefings, and collaborate with the Joint Staff to ensure the Department is effectively organized to address evolving threats and support the warfighter.

71. If confirmed, how will you engage with the National Telecommunications and Information Administration (NTIA) to ensure protection of spectrum bands critical to warfighting operations?

If confirmed, I look forward to engaging regularly with the NTIA Administrator to ensure she is fully informed of the potential impact of spectrum repurposing decisions on warfighting operations.

72. In your opinion, what are your thoughts on sharing technology as a unique solution to satisfying the demands for spectrum? If confirmed, how would you prioritize investments into these technologies?

Advanced spectrum sharing is vital to America's technological competitiveness and is the best means to increase commercial spectrum access while preserving our warfighter's access to spectrum for homeland defense and national security. If confirmed, I will work closely with industry and others in government to develop the technologies necessary to make advanced spectrum coexistence a reality.

73. What are your views regarding the auction, for non-federal use, of the 3.1-3.45 GHz and 7-8 GHz spectrum bands?

My understanding is Congress has excluded 3.1-3.4 GHz and 7.4-8.4 GHz from auction through 2034 in the One Big Beautiful Bill in recognition of their critical importance to homeland defense and national security. If confirmed, I look forward to a classified briefing to learn more about critical systems in those bands that support our warfighter.

Positioning, Navigation, and Timing

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

Some of the biggest challenges include adversary jamming, spoofing and denial of GPS signals, as well as the need to provide assured PNT capabilities for warfighters operating in contested or denied environments. If confirmed, I will prioritize synchronizing the space, control, and user segments of the GPS system to ensure reliable warfighter capability. I will also focus on accelerating the development and integration of alternative PNT solutions to address both external threats and internal modernization challenges.

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

If confirmed, I will prioritize addressing immediate PNT challenges by advancing policies, technologies, and procedures to counter adversary threats and integrate non-GPS solutions. In the long term, I will focus on delivering a resilient mix of modernized GPS and alternative PNT capabilities to meet the Joint Force's needs efficiently and effectively.

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

If confirmed, I will prioritize the development and fielding of alternative PNT solutions to ensure resilient capabilities when GPS is degraded or denied. While modernization efforts are underway, I will work with the Services to identify and resource viable near- and far-term solutions, ensuring we focus on high-impact, military-grade innovations to support the Joint Force.

Command, Control, and Communications

77. In your view, what is the role of the CIO regarding warfighting networks that provide command and control of our armed forces, as compared to the CIO's role regarding infrastructure and networks? Does your authority extend to warfighting networks and systems in the Department?

In my view, the Department's CIO must ensure its customers (primarily the warfighter) have resilient access to the core IT and communication services within the Department's Information Network. For warfighting, this requires a command, control, and communication architecture that closes with warfighters and their platforms in sometimes austere and contested environments with little or no existing infrastructure or networks. If confirmed, I would have the statutory authority to guide enterprise architecture, set Department-wide IT and cybersecurity standards, and certify the Department's IT budget process.

78. 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, a major challenge facing the Department's C3 programs is accelerating the development and integration of IT systems into modern warfighting platforms while ensuring interoperability and cyber resilience. If confirmed, I look forward to working with my USW(R&E) and USW(A&S) colleagues to pursue innovative, common-sense approaches to speed this process.

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

If confirmed, I will assess the Department's C3 resiliency to ensure we can outpace near-peer adversaries like China and Russia, who are rapidly advancing their cyber and space-based capabilities. I will prioritize leveraging our unmatched defense industrial base and commercial space industry to build resilient systems with diverse communication and PNT options to reduce reliance on GPS.

80. There has been much discussion about the importance of networking and connecting warfighting capabilities across air, land, and sea platforms. If confirmed, what would you do to facilitate development and implementation of Combined Joint All Domain Command and Control concepts?

If confirmed, I will prioritize the development of secure, interoperable networks and data standards to enable seamless connectivity across air, land, sea, space, and cyber domains. I will work closely with the Services and allies to align architectures, adopt open standards, and ensure data can flow securely and in real time to support Combined Joint All-Domain Command and Control (CJADC2). By fostering collaboration and leveraging emerging technologies to enhance decision-making and deliver a decisive advantage to the warfighter.

81. Please describe your view of the CIO's role with respect to overseeing the cryptographic accounts at the National Security Agency (NSA) and recent efforts with respect to cryptographic modernization?

The CIO ensures cryptographic modernization efforts are synchronized enterprise-wide and that investments are prioritized to meet the operational needs of today's warfighters. Additionally, the CIO coordinates with the NSA and DoW Components to oversee, review, and assess communications security initiatives. This ensures the Department maintains its technological edge and strong security posture.

Information Technology Workforce and the Cyber Excepted Service

The Chief Information Officer serves as the functional community manager for 72 civilian occupational specialties, which account for approximately 52,000 civilian employees. Additionally, the CIO is one of the chairs of the Cyber Workforce Management Board, which oversees the management of the entire Department of Defense military and civilian cyber workforce. These are critical roles as the Department develops its employment practices to attract and retain personnel with highly valuable information technology and cyber-related skillsets.

82. **As you shape and guide the Department's cyber and IT workforce, how do you determine whether a certain position should be filled by military, civilian, or contractor personnel?**

    The DoW CIO's role is to work with the Military Departments and other DoD Components to help define cyber workforce position qualification and proficiency requirements including the tasks, knowledge, skills, and abilities required to perform each work role. Components determine the appropriate workforce mix of civilian, military, and contractor personnel consistent with law and policy.

83. **Each military Department and DOD Component competes for the same set of skilled and experienced employees, who are highly skilled and experienced in cyber and information technology. If confirmed, how will you work through the Cyber Workforce Management Board to de-conflict and prioritize personnel requirements across the Department to ensure the strategic allocation of manpower?**

    If confirmed, I will ensure that I am informed on the status of cyber workforce readiness, skill sets, and pipeline, and will leverage data, industry insights, and cross Department collaboration to drive decision-making for human capital management. This will enable cyber leaders to prioritize actions across the DoW and determine actions that mitigate suboptimization of the cyber talent management lifecycle process.

84. **The DOD CIO issued the Defense Cyberspace Workforce Framework (DCWF) in February 2023, establishing a comprehensive structure for the cyber workforce. How would you leverage this relatively new framework to better align workforce development efforts with evolving mission requirements, particularly with respect to emerging technologies like artificial intelligence and quantum computing?**

    If confirmed, I would collaborate across functional communities to further expand the DCWF, incorporating emerging technologies like electromagnetic spectrum and quantum computing, and further incorporating artificial intelligence.

85. **The February 2023 DOD 8140 policy replaced the previous 8570 policy series**

and expanded the scope of cyber workforce qualification requirements. If confirmed, what actions will you take to fully implement this policy by the February 2026 tracking deadline?

My understanding is the DoW Office of the CIO is on track to implement the policy. If confirmed, I will assess the progress of DoW 8140 requirements and work to ensure efforts to implement this policy by the deadline remain a top priority for the Department.

86. The DoD 8140 policy identifies 72 distinct work roles across the cyber workforce. If confirmed, how would you ensure that training and certification requirements across these roles remain current with rapidly evolving technology and threat landscapes?

The evolving Defense Cyber Workforce Framework encompasses more than 72 work roles, necessitating continuous reassessment of education, training, and certifications to ensure skills proficiency. If confirmed, I will leverage expertise across government, industry, and academia to close skills gaps, prioritizing challenging real-world exercises, simulations, and AI-based tools to develop a realistically trained cyber workforce.

The FY 2016 NDAA authorized Cyber Excepted Service (CES) for the DoD. While significant progress has been made in implementing needed support for these civilians, there is much more to do in the years to come to fully take advantage of the benefits of this program.

87. The Department has been working to expand the CES from approximately 15,000 positions to potentially 75,000 positions. If confirmed, what is your vision for this expansion, and how would you ensure it complements rather than conflicts with other personnel systems within DoD?

If confirmed, my vision for expanding the Cyber Excepted Service is to strengthen our ability to attract and retain world-class cyber talent while ensuring it complements — not competes with — other personnel systems. CES expansion must be strategic and proactive, filling true capability gaps where hiring flexibilities are needed most. I would prioritize mobility and career pathways across all personnel systems, supported by clear governance and transparency, so that employees can grow without barriers. CES should be a force multiplier for the mission and a seamless part of the larger DoW workforce.

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

In my view, three obstacles hinder full implementation of CES: (1) inconsistent messaging, (2) complex governance, and (3) workforce concerns. If confirmed, I will address these challenges by clarifying CES's purpose and advantages, streamlining governance for ease of adoption by components, and providing transparency and mobility for the workforce. My goal is to build trust and ensure CES strengthens the Department's ability to attract and retain top cyber talent.

89. In your judgement, what additional authority does the Department need to help further recruit and retain talent to the CES? If confirmed, how will you work with Congress to develop and authorize those policies?

If confirmed, I would work with Department leadership to develop proposed authorities that are data-driven, implementable, and clearly tied to mission needs. In addition, I would engage regularly with Congress to share lessons learned, strengths, and opportunities for improvement.

90. 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?

Both quantitative (time-to-hire, fill rates, retention, salary competitiveness) and qualitative (employee engagement, career mobility, mission readiness, innovation aptitude) metrics are essential for assessing the effectiveness of the Cyber Excepted Service. If confirmed, I will ensure regular review and transparent reporting of metric data to inform potential adjustments to CES, ensuring it remains both effective and accountable in attracting world-class cyber talent.

Science, Technology, and Innovation

The Department of Defense has identified 14 critical technology areas that are essential for maintaining U.S. military and technological superiority. These areas, outlined by the Office of the Under Secretary of Defense for Research and Engineering, include: biotechnology, quantum science, future generation wireless technology (FutureG), advanced materials, trusted AI and autonomy, integrated network systems-of-systems, microelectronics, space technology, renewable energy generation and storage, advanced computing and software, human-machine interfaces, directed energy, hypersonics, and integrated sensing and cyber. The DoD has prioritized these technologies for focused investment and development as they represent capabilities that will be crucial for national security in the coming decades.

91. The DoD has identified 14 critical technology areas, including advanced computing and software, artificial intelligence, quantum science, and microelectronics. If confirmed, how would you ensure the Department's information technology infrastructure and policies enable rather than hinder innovation in these critical areas?

If confirmed, I will prioritize the Department’s IT infrastructure security, adaptability, and optimization, supporting rapid innovation in critical technology areas. I will prioritize streamlining policies, implementing zero trust principles, and implementing a risk-based approach to accelerate the development and deployment of emerging technologies like AI, quantum science, and microelectronics, while maintaining mission security and integrity.

92. From your perspective, what is the most optimal way to address the cybersecurity challenges associated with collaborative research and development across military, academic, and private sector partners while maintaining appropriate security controls?

If confirmed, I will prioritize establishing a unified framework that ensures all participants adhere to baseline cybersecurity standards while enabling secure collaboration. Strengthening interoperability, risk management, Zero Trust principles like identity management and access controls, threat intelligence sharing, and continuous threat monitoring will be key to protecting sensitive data and rapidly advancing innovation without compromising security.

93. Advanced computing and software technologies are evolving rapidly, with the DoD acknowledging that "the speed at which software develops outpaces the Department's ability to stay up to date." If confirmed, what specific strategies would you implement to close this gap?

The Department must field secure software at the speed of relevance, which requires changes in how it governs, acquires, and operates software. If confirmed, I will focus on strategies such as institutionalizing continuous Authority to Operate through automated compliance, aligning acquisition to prioritize modularity and outcomes, driving interoperability requirements, and standardizing a secure software supply chain with tools like software bills of materials. These efforts would reduce cyber risk, accelerate delivery, and ensure innovations reach the warfighter faster and more effectively.

94. Open Radio Access Network (O-RAN) initiatives have been a significant focus of DoD's 5G strategy to promote interoperability and reduce dependence on single vendors. If confirmed, would you advance these efforts to ensure secure, resilient, and interoperable wireless communications for the warfighter?

If confirmed, I will support Open RAN initiatives to enhance secure, resilient, and interoperable 5G communications for the warfighter. I will prioritize rigorous testing, cybersecurity standards, and partnerships with trusted vendors and allies to ensure these technologies are secure and reliable while reducing dependence on untrusted suppliers.

95. What is your familiarity with the use of formal methods approaches to mathematically validate and verify the security of IT software and hardware?

What role do you think DOD should play in fostering the use of formal methods more broadly across the IT ecosystem?

I am familiar with formal and informal methods, such as SBOM validations, code scanning, hardware and firmware inspection, identity assessment, to name a few. These and other methods include mathematical approaches, to validating security, particularly in critical areas like cryptography and operating system kernels. If confirmed, I will support targeted use of formal methods where they provide the most value, while fostering broader adoption through research, standards, and collaboration with industry. I will also prioritize integrating technologies which provide Security Posture Management to enhance security visibility and strengthen cybersecurity across operational environments.

Congressional Oversight

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.

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

Yes.

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

Yes.

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

Yes.

99. Do you agree, without qualification, if confirmed, to keep this committee, its subcommittees, other appropriate committees of Congress, and their respective

staffs appraises new information that materially impacts the accuracy of testimony, briefings, reports, records—including documents and electronic communications, and other information you or your organization previously provided? Please answer with a simple yes or no.

Yes.

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

Yes.

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

Yes.

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

Yes.