Senate Armed Services Committee
Advance Policy Questions for Dr. Michael Sulmeyer
Nominee to be Assistant Secretary of Defense
for Cyber Policy

Duties and Qualifications

Section 901(a) of the James M. Inhofe National Defense Authorization Act (NDAA) for Fiscal Year 2023 (Public Law 117-263) created the position of the Assistant Secretary of Defense for Cyber Policy (ASD(CP)) whose principal duty "shall be the overall supervision of policy of the Department of Defense for cyber." You are the first person nominated to serve in this position.

1. **What is your understanding of the duties and responsibilities of the ASD(CP)?**

   The ASD(CP) is the senior official responsible for the overall supervision of DoD policy for cyber issues as specified in 10 U.S.C. § 138 and is the Principal Cyber Advisor to the Secretary of Defense as described in 10 U.S.C. § 392a. The ASD(CP) will oversee two subordinate offices: the Office of the Deputy Assistant Secretary of Defense for Cyber Policy (DASD Cyber Policy) and the Office of the Principal Cyber Advisor (OPCA).

2. **If confirmed, what additional duties and responsibilities do you expect the Under Secretary of Defense for Policy to prescribe for you?**

   In standing up this office, the Department of Defense's leadership is giving cyber issues the focus and attention that Congress intended. The ASD(CP) position provides an opportunity to streamline the evaluation and oversight of the policies, programs, and strategies that enable DoD cyber operations. I understand the ASD(CP) also has responsibilities for certain electronic warfare topics that relate closely to cyber operations. If confirmed, I would anticipate an early discussion with the Under Secretary for Policy regarding other potential additional duties and responsibilities.

3. **What background, experience, and expertise do you possess that qualify you to serve as the ASD(CP)?**

   I have served in various roles in and outside of government advising on cyber matters, most recently as the Principal Cyber Advisor to the Secretary of the Army. In that role created by Congress, I provide advice on a range of cyber issues to the Secretary of the Army. Previously, I worked at U.S. Cyber Command on several strategic and operational matters. Prior to those roles within government, I spent time in academia as the Director of the Cybersecurity Project at the Harvard Kennedy School's Belfer Center for Science and International Affairs.

4. **What leadership and management experience do you possess, both in the private sector and in government, that you would apply to your service as ASD(CP), if confirmed?**

From my time in academia, I built and managed a team of cyber policy researchers. I developed a recruiting strategy. I successfully persuaded administrators of the need to pay these researchers at higher bands given the scarcity of this kind of analytic talent. I mentored their research and supported their professional development. From my time with the Army, I utilized hiring and other recruiting and retention authorities to recruit and retain a team to assist with advising Army leadership on cyber issues. I looked for advisors who could complement my experience with their own, such as warrant officers and enlisted advisors with more direct operational experience. From these and other experiences, I also learned the value of continuing education for myself and my colleagues and peers. If confirmed, I would dedicate time to the professional development of those who work in the office of the ASD(CP).

Major Challenges and Priorities

5. **In your view, what are the major challenges that will confront the ASD(CP)?**

In my view, the first major challenge will be the cyber activities of People's Republic of China, which is the pacing challenge for the Department of Defense. They use cyber operations to attempt to gain political, military, and economic advantages. The malicious cyber threats posed by the Russian Federation will be another major challenge for the ASD(CP). The Department of Defense must also remain vigilant against cyber threats posed by Iran, North Korea, and non-state entities. Protecting our critical infrastructure and our most sensitive data from these actors are critical priorities. To do so, I will focus on strengthening our people, technology, and partnerships.

6. **If confirmed, what plans would you implement to address each of these challenges?**

If confirmed, my principal goal will be to generate the combat power and sustained readiness in cyberspace necessary to advance and defend American interests from current and future threats. To achieve this objective, I would begin by accelerating U.S. Cyber Command's efforts to meet and defeat threats to our nation. I would do so in close partnership with the Commander of U.S. Cyber Command, General Haugh. I would also focus on supporting the personnel who execute and provide integral support to our mission, including military and civilian, active, Guard, and Reserve, as well as our partners in academia and industry. We must retain and recruit the nation's top talent to deter, and when necessary, defeat our adversaries. I would then turn to our capability development to understand ways to expedite delivery of innovative technology to our operators. Finally, I would ensure the Department of Defense is poised to expand the partnerships we need to both fortify the Department's cybersecurity and to make the most of our nation's advantages in artificial intelligence and emerging technologies.

7. **If confirmed, what broad priorities would you establish for your tenure in office?**

   If confirmed, I would prioritize the evaluation of force-generation models to determine the most effective and efficient approaches to build combat power and sustained readiness to defend the nation from cyber threats. I would look forward to working closely with General Haugh, Commander of U.S. Cyber Command, to ensure U.S. Cyber Command is successful in executing its service-like authorities, including the enhanced budget authorities recently granted to U.S. Cyber Command by Congress.

Civilian Control of the Military

Congress created the position of ASD(CP) to ensure civilian oversight of the growing Cyber Operations Forces under U.S. Cyber Command. Much like U.S. Special Operations Command (SOCOM), which has service-like roles and responsibilities, it is necessary to provide a service secretary-like civilian role to help advocate for those forces, and to ensure that civilian control.

8. **What are your views on the purposes underpinning creation of the position of the ASD(CP) and how would you effectuate those purposes, if confirmed?**

   In my view, when Congress directed the creation of an ASD(CP) in the FY 2023 NDAA, it signaled an increased emphasis on the importance of cyber issues and the need for a more senior level of representation and advocacy for those issues in the Department of Defense. The creation of the ASD(CP) follows the civil-military relationship from special operations: a civilian Assistant Secretary of Defense overseeing and working collaboratively with a uniformed Combatant Commander to generate outcomes that improve the defense of the nation. In addition, elevating the prominence of cyber issues to the Assistant Secretary level should enable greater unity of effort across the military departments and multiple OSD components that have equities in cyber issues. There should also be opportunities to promote efficiencies by taking a whole-of-Department view of cyber operations resources. If confirmed, I will work across the services, the Office of the Secretary of Defense, and the Joint Staff to ensure proper oversight of cyber operations, forces, and budgets. I also commit to working with Congress to promote transparency and ensure timely responses on cyber matters.

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

   To fulfill the requirement for civilian control of the Armed Forces related to cyberspace, I would begin by working with the Secretary and Deputy Secretary of Defense, as well as the Undersecretary of Defense for Policy, to ensure a clear articulation of the civilian policy goals. I would then work with the Commander of U.S. Cyber Command to ensure the Commander has the resources and authorities to execute his assigned missions that reflect those policy goals. I would also ensure those civilian policy goals are reflected in the Command's resourcing foundations, such as its new enhanced budget authorities.

Finally, I would look to other models, such as the relationship between the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict and the Commander of U.S. Special Operations Command, to understand lessons learned from their civil-military relationship.

Cyber Policy and Authorities

10. What do you see as the primary cyber policy challenges currently facing the Department of Defense, and what suggestions do you have for addressing them?

In my view, the People's Republic of China, which seeks to exploit vulnerabilities to undermine our military's competitive edge, is the pacing challenge and the primary cyber policy challenge facing the Department of Defense. Russia and its malicious cyber activities pose an acute threat to the Department. Iran, North Korea, and non-state actors also aim to use cyber operations in ways that are counter to our interests. As we defend against those foreign challenges, a key cyber policy challenge at home is recruiting and retaining a top workforce, developing capabilities with the latest technology, and forming lasting partnerships with industry, academia, and allies and partners.

If confirmed, in partnership with the Commander of U.S. Cyber Command, I will prioritize generating the combat power and sustained readiness in cyberspace to deter, defend against, and defeat threats to our nation. I will also explore how advances in artificial intelligence can better enable our warfighters to execute their missions.

11. If confirmed, what would your relationship be with:

- **The Commander of U.S. Cyber Command:** The Commander of U.S. Cyber Command is responsible for the planning and execution of military cyber missions; serving as the cyber operations joint force provider and joint force trainer. If confirmed, I look forward to working closely with the Commander of U.S. Cyber Command on all policy issues affecting the Command's ability to achieve national security objectives.

- **The DOD Chief Information Officer:** The DoD Chief Information Officer (DoD CIO) is the principal staff assistant and senior advisor to the Secretary of Defense and Deputy Secretary of Defense for all matters relating to the DoD information enterprise including cybersecurity, communications, and information systems. If confirmed, I intend to foster a close relationship with the DoD CIO to strengthen governance of cybersecurity, communications, information systems, and spectrum matters.

- **The Military Service Principal Cyber Advisors:** These Principal Cyber Advisors (PCAs) address cyber readiness, capabilities, budget, and strategy for their respective military departments. If confirmed, I will work closely with the PCAs on developing and implementing policies and strategies to synchronize these efforts across the Department of Defense.

- **The DOD Chief Digital and Artificial Intelligence Officer:** The Chief Digital and Artificial Intelligence Office (CDAO) is DoD's senior official responsible for leading the acceleration of DoD's adoption of data, analytics, and AI to generate decision advantage. If confirmed, I look forward to working closely with the CDAO, in coordination with other DoD and OSD component heads, to integrate efforts on data, analytics, and AI adoption to build enduring advantage for the Department of Defense and the nation.

- **The Director for the Defense Advanced Research Projects Agency:** The Defense Advanced Research Projects Agency (DARPA) enables pivotal investments in breakthrough technologies for national security. If confirmed, I look forward to working with DARPA and U.S. Cyber Command to mature and transition new cyber capabilities to the operational warfighter that will enable full spectrum cyber operations.

- **The Director of Cybersecurity and Infrastructure Security Agency (CISA) at DHS:** The DoD's relationship with the Department of Homeland Security is imperative to ensuring the cybersecurity of U.S. critical infrastructure systems. If confirmed, I will prioritize expanded coordination and communication between our two Departments on cyber matters. I will also ensure DoD is postured to address requests for assistance from the Department of Homeland Security and other Federal civilian agencies.

- **The Director for the Defense Cyber Crime Center:** The Defense Cyber Crime Center is a Federal Cyber Center, and the Office of the Under Secretary of Defense for Policy fulfills the Department of Defense's role as the Sector Risk Management Agency of the Defense Industrial Base (DIB). Both roles share responsibility for protecting critical infrastructure. If confirmed, I will ensure that we are fully aligned in efforts to protect the DIB from malicious cyber activity.

- **The White House Office of the National Cyber Director:** The National Cyber Director is the principal advisor to the President on cybersecurity policy and strategy and leads whole-of-government coordination of programs and policies to improve the cybersecurity posture of the United States, increase information and communications technology security, understand and deter malicious cyber activity, and advance diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace, among other matters. If confirmed, I look forward to working with the Office of the National Cyber Director to support the strategic approach outlined in the 2023 National Cybersecurity Strategy including aligning DoD efforts to deter and disrupt cyber threat actors and building enduring advantage for the nation in cyberspace.

- **The Director of the Defense Intelligence Agency:** The Director of the Defense Intelligence Agency (DIA) manages and executes specified Defense Intelligence and counterintelligence functions across the Defense Intelligence Enterprise and for select functions across the greater Intelligence Community. As a combat support agency and element of the Intelligence Community, DIA analyzes and disseminates military intelligence in support of military missions and serves as the nation's primary manager and producer of foreign military intelligence. If confirmed, I look forward to working closely with the DIA Director to ensure the availability of timely and actionable intelligence in support of cyber operations and exploring the intersection of emerging technologies and cyber capabilities, in line with the 2023 DoD Cyber Strategy.

Given the difficulty in anticipating and defending against cyber attacks, many suggest that the Department of Defense can only rely on a policy of cyber deterrence to protect its and the Nation's critical systems.

12. Do you believe that deterrence is possible in cyberspace? In your view, is the current level and tempo of cyber attacks on the Department and on the Nation tolerable?

Cyber operations can contribute to deterrence objectives, especially when used with other instruments of national power. Cyber capabilities are most effective when employed as part of a whole-of-government approach to convince potential adversaries that the costs of their hostile activities outweigh their benefits. This entails the integration of military and non-military capabilities as well as integration across regions, across the spectrum of conflict, across the U.S. government, and with allies and partners. To reduce the incidence of malicious cyber activity, cost imposition approaches to deterrence should be integrated with bolstering cyber defenses.

13. Do you believe that the Department's current capabilities and policies allow for the maintenance of robust cyber deterrence?

Strong cyber capabilities, as well as other instruments of national power, can provide an integrated approach to deterrence and make for a more credible posture to defend the nation. In addition, defending forward by challenging and contesting the actions of our competitors and adversaries below the level of armed conflict sends an important signal that the Department of Defense has a variety of mechanisms at its disposal to disrupt cyber threats. If confirmed, I look forward to working with the committee to bolster the foundations of this deterrence posture, such as through improved foundational intelligence and rapid capability development and acquisition.

14. How can the Department improve its cyber deterrence posture?

In my view, the Department of Defense's cyber deterrence posture supports the strategic objectives defined in the 2023 DoD Cyber Strategy. If confirmed, I would work with the Commander of U.S. Cyber Command to generate the combat power and sustained readiness for our cyber operations forces to provide cyber options to Department of Defense leadership. I would also work with other counterparts to ensure those capabilities are integrated with non-cyber capabilities as well. We can further support these efforts by ensuring a more resilient DoD Information Network and by enabling the defense of non-Department of Defense networks, including industry partners and allies.

15. Do you believe that the Department possesses the necessary authorities to stand up an effective cyber deterrence posture?

From what I understand, I believe that the Department of Defense possesses the necessary authorities. However, if confirmed, and if I determine that certain authorities could make for a more effective cyber deterrence posture, I would advocate for them with my leadership and this committee.

16. What are your views on the relationship between space, cyber space, and nuclear escalation in the context of our Nation's strategic posture?

The relationship between space, cyberspace, and nuclear escalation is important for many reasons, especially to manage the risk of potential escalation of threats and actions across domains. Cyber actions may not always be met with cyber responses, so it is imperative that our leaders see across these domains to manage escalation especially in a crisis. If confirmed, I look forward to working with the ASD for Space Policy, the U.S. Space Force, U.S. Strategic Command, and industry to strengthen our nation's strategic posture.

17. What is your view of the appropriate relationship and division of responsibility between the Commander, NORTHCOM, and the Commander, CYBERCOM, with respect to cyber support to civil authorities?

The Commander of U.S. Northern Command is the primary Combatant Commander responsible for defense of the homeland and plays the role of coordinating defense support to civil authorities. While U.S. Cyber Command can, in exigent circumstances, be called upon under that authority to support missions domestically, its primary roles in defense of the homeland are to defend forward, prevent, and disrupt foreign cyber attacks, and respond overseas to domestic cyber events. Due to the Department of Defense's limited authority to address risks outside DoD facilities, coordination between U.S. Northern Command, U.S. Cyber Command, and the Department of Homeland Security is essential to protecting critical infrastructure.

18. What role do you foresee your office having in helping shape international norms of behavior, such as through efforts like the updating of the Tallinn Manual?

In my view, the Department of Defense, including the office of ASD(CP), helps to shape and reinforce norms of responsible state behavior in cyberspace. If confirmed, I would position the office to support the Department of State's leadership in building consensus on cyber norms, including by working with U.S. departments and agencies to expose and publicly attribute behavior inconsistent with those norms.

I view the Tallinn Manual as an informative product. If confirmed, I would consider such products as important reference material for understanding the application of international law to cyber operations. However, they would not provide authoritative or binding direction. Developments in cyberspace occur at a rapid and continuous pace. I therefore support efforts to generate updated research material that the leaders at the Department of Defense may consult.

The National Defense Authorization Act for Fiscal Year 2021 established the position of National Cyber Director (NCD) to improve coordination and integration across the government in developing cyberspace strategy, policy, plans, and resource allocation.

19. What is your understanding of how DOD has been supporting the National Cyber Director?

I understand that the Department of Defense has supported the National Cyber Director (NCD) efforts to develop and implement the National Cyber Strategy. DoD's role in that strategy includes disrupting and dismantling cyber threats by incorporating cyber operations into campaigns that aim to defend the nation in cyberspace. I further understand that DoD supports NCD's efforts to engage with industry and international stakeholders, as well as coordinating on other interagency initiatives.

20. Do you have suggestions for how you might improve the relationship with the NCD if confirmed?

If confirmed, I would prioritize maintaining a strong partnership between the Department of Defense and the NCD, with particular focus on implementing the 2023 DoD Cyber Strategy and ensuring its alignment with implementation of the 2023 National Cybersecurity Strategy. I am committed to enhancing ongoing collaboration efforts between our organizations and contributing to NCD-led whole-of-government efforts to engage with private sector, international, and other non-Federal stakeholders. I am particularly interested in efforts by NCD to recruit and retain cyber talent in public service, and if confirmed I look forward to supporting those efforts from a Department of Defense perspective.

Cyber notifications from the Department for sensitive cyber military operations, as required by law, have become increasingly vague and do not provide enough information for the committee to perform adequate oversight of these operations.

21. If confirmed, what would you do to improve these cyber operations notifications?

I consider transparency with Congress to be a top priority and understand the Department of Defense has multiple mechanisms by which to convey information on sensitive military cyber operations to the defense committees. If confirmed, I will review these notifications and I will work with the defense committees to address any concerns about the nature and content of written notifications, ensuring the Department provides sufficient information for effective Congressional oversight.

22. Are there steps other than improving the written notifications that you would take, if confirmed, to help Congress perform oversight of these critical operations?

I consider it imperative to communicate with Congress frequently and through multiple forums. I will ensure the Department of Defense maintains regular engagements on cyber issues with Congress, including DoD's statutory responsibility for quarterly operations briefings, and I will provide regular updates on military activities and operations in cyberspace.

23. What is your understanding of the process for how the Department might respond to a request for Defense Support to Civilian Authorities (DSCA) when it comes to cyber incident?

I understand DoD provides reimbursable Defense Support of Civil Authorities (DSCA) in support of a lead Federal agency when directed by the President or when the Secretary of Defense has approved a request for assistance pursuant to the Stafford Act or the Economy Act. DSCA is typically requested by a lead Federal agency in response to a crisis or natural disaster, or in support of special events, when Federal, State, local, tribal, and territorial capabilities are overwhelmed, exhausted, or when DoD has military-unique capabilities that are needed. Pursuant to Presidential Policy Directive 41 (PPD-41), the lead Federal agencies for cyber incident response are the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). If confirmed, I would support the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs in reviewing any requests pertaining to cyber resources that are received. I would also seek an early discussion with DHS and FBI to proactively identify efficient and effective mechanisms to respond to requests for DSCA when it comes to cyber incidents.

Enhanced Budget Control (EBC)

U.S. CYBERCOM was given enhanced budget control (EBC) authority under Section 1507 of the National Defense Authorization Act for Fiscal Year 2022, but the authority did not take full effect until the FY 2024 Further Consolidated Appropriations Act was passed earlier this year. As stated by General Haugh in testimony earlier this year "The Enhanced Budgetary Control authority granted by Congress is transformational for the Command. When fully implemented with our FY24 appropriation to U.S. CYBERCOM, it entrusts more than $2 billion in DOD budget authorities to U.S. CYBERCOM and

streamlines how we engage the Department's processes. EBC is already paying dividends in the form of tighter alignments between authorities, responsibility, and accountability in cyberspace operations. Greater accountability, in turn, facilitates faster development and fielding of capabilities."

24. If confirmed, how do you intend to maintain better reporting and oversight over the portion of funding under EBC, as well as those areas outside of EBC that are retained by the service and defense agencies?

In addition to EBC oversight of U.S. Cyber Command's Planning, Programming, Budgeting, and Execution activities, the Principal Cyber Advisor (PCA) to the Secretary of Defense is responsible for reviewing each proposed budget transmitted by the services and defense agencies and certifying to the Secretary of Defense the budget adequacy for cyber operations, as specified in 10 U.S.C § 392a and section 1501 of the National Defense Authorization Act for Fiscal Year 2023.

If confirmed, I will coordinate with the Comptroller and Office of Cost Assessment and Program Evaluation to identify opportunities to improve the PCA's role in the Department's PPBE process. I will work closely with the Commander of U.S. Cyber Command, as well as the Service Secretaries and heads of the defense agencies with resources aligned to the cyber operations portfolio, to issue guidance for the future years defense plan and build a strong team to help me improve the reporting and oversight of funding.

One area not included in EBC was service cyber science and technology efforts. There is some concern that has been raised that with the full implementation of EBC, that the services will not continue robust service investments in cyber science & technology (S&T).

25. How will you implement processes to try to retain insight and advocate for service-level cyber S&T investments in the future years defense plan?

S&T investments are a critical enabler of the acquisition community and operational forces. This is especially true in the cyber operations community, where the Defense Advanced Research Projects Agency (DARPA), the Strategic Capabilities Office (SCO), and the service labs have consistently developed technologies used in military operations in cyberspace. If confirmed, I will work with the Military Department Principal Cyber Advisors and other leaders to identify and support areas where service-sponsored S&T funding adds a competitive advantage for the Department's cyber posture. I will also coordinate with USD(R&E), DARPA, and SCO to advocate for the appropriate investments through annual programming guidance for the future years defense plan to enhance cyber capabilities across the Department of Defense.

Developing and Coordinating Whole-of-Government Information Operations Policy and Strategy

Effective operations in the information environment require not only integration across all the organizations in DOD with responsibilities for components of information operations, but also across the whole government.

26. In your view, does the United States have an effective "whole-of-government" approach to combatting hostile information operations directed against the United States, its allies, and interests?

I understand that the Department of Defense works closely with partners across the U.S. government to identify and combat information operations directed against the United States, our allies, and interests by our adversaries. Combatting these operations involves using a range of instruments of national power to disrupt their activities. If confirmed, I look forward to supporting the Department of Defense and partner agencies to protect the United States, our allies, and our interest against adversary information operations.

In the cyber domain, Congress has enacted legislation clarifying that cyber operations can be conducted as traditional military activities. The administration has adopted streamlined processes for review and approval of cyber operations, which has expedited decision-making, but has retained appropriate vetting of sensitive operations.

27. What is your assessment of DOD's ability to conduct effective military operations in the information environment to defend U.S. interests against malign influence activities carried out by state and non-state actors?

From what I understand, I believe that the Department of Defense has the necessary authorities and capabilities to conduct effective military operations in the information environment, including for cyber operations. If confirmed, I would prioritize ensuring DoD maintains and matures its ability to operate in the information environment.

28. In your view, is responsibility for Information Operations clearly delineated and properly situated within the military services and the Department?

I understand that the Under Secretary of Defense for Policy has been designated the DoD Principal Information Operations Advisor (PIOA) and is responsible for the oversight of policy, strategy, planning, resource management, operational considerations, personnel, and technology development across all the elements of information operations of the Department. If confirmed, I will work closely with the PIOA on cyber-related issues.

29. Do you believe the Department has a mature strategic concept for such efforts that is integrated with all of the other elements of information power, like cyber, electronic warfare, and military deception?

I understand that the Secretary of Defense signed the Strategy for Operations in the Information Environment in November 2023, which identifies four lines of effort to enable the Department of Defense to fully integrate and modernize information operations with other elements of information power. If confirmed, I look forward to contributing to the implementation of this strategy.

30. What is your assessment of the metrics used to assess effectiveness of DOD information operations?

I understand that the Principal Information Operations Advisor, through the Office of Information Operations Policy, is responsible for developing and refining effectiveness metrics for DoD information operations. If confirmed, I look forward to working with the PIOA to learn more about these metrics and the best practices for assessing the effectiveness of DoD information operations.

31. Does DOD have sufficient authorities and resources to conduct these operations effectively? If not, what additional authorities and resources would you request, if confirmed?

At this time, I do not envision a need for additional cyber operations authorities for DoD cyber operations. However, if confirmed, I will continue to monitor whether additional responsibilities or authorities will materially improve the Department of Defense's and U.S. Cyber Command's ability to execute its missions and I will communicate any findings I might have to the Secretary and to Congress.

32. What is your understanding of the relationship between the Principal Cyber Advisor (PCA) and the Principal Information Operations Advisor (PIOA), between the cyber mission and the information operations mission, and between the DOD components assigned to execute the two missions?

I understand that the Principal Cyber Advisor and the Principal Information Operations Advisor work closely together to ensure the synchronization of policy and oversight for DoD cyber and information operations, and that this close coordination is replicated within the DoD components assigned to execute the two missions. If confirmed, I look forward to understanding more about how these OSD and operational components can continue to support each other to improve the execution of these two missions.

In the Defense Department, CYBERCOM is focused on technical cyber missions and skills, while different organizations are responsible for information operations, psychological and deception operations, and electronic warfare. In addition, there are concerns that DOD's focus on tactical and operational support to deployed forces has resulted in neglect of strategic-level information operations.

33. What are your views as to whether CYBERCOM should be assigned responsibility for information operations in addition to cyber operations, especially considering that CYBERCOM has to date focused on tactical operations to support the specific cyber mission, and the linguistic and cultural expertise in the Department needed to craft strategy for information operations do not reside in CYBERCOM?

In my view, cyber and information operations are often complementary. If confirmed, I would examine how the current assigned responsibilities have evolved and how they align against current and future threats. My goal will be to ensure that the Department of Defense is getting as much of a return on its investments in these areas as possible to further the defense of the nation. If after review I believe that certain adjustments would materially improve U.S. Cyber Command's ability to execute its mission, I will communicate those to the Secretary and to Congress.

Dual Hatting of Commander, CYBERCOM

34. In your view, should the arrangement whereby the Commander, CYBERCOM is "dual-hatted" as the Director of the National Security Agency (NSA) be maintained, modified, or ended? Please explain your answer.

I support maintaining the Dual Hat leadership arrangement. In May 2023, the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Director of National Intelligence conveyed to Congress their agreement that retaining the Dual Hat leadership arrangement is in the best interest of national security. U.S. Cyber Command and NSA deliver critical capabilities against our pacing challenge and other key national security concerns as identified in the National Defense Strategy. The Dual Hat leadership arrangement has been integral to their success on many topics, such as protecting National Security Systems, enabling partners in the Defense Industrial Base with better cybersecurity, and election defense from foreign interference. Ending the Dual-Hat leadership arrangement would increase risk to critical work undertaken at both NSA and at U.S. Cyber Command. DoD and the Office of the Director of National Intelligence continue to work together to strengthen and maintain an enduring Dual Hat arrangement that ensures the best outcomes for the nation regarding both cyber operations and intelligence activities.

35. What mechanisms are in place to ensure that the missions of CYBERCOM and NSA are mutually supporting and do not inadvertently draw resources from one important mission or the other?

A series of support agreements, memoranda of understanding, and special partnership agreements ensure that the separate roles, resources, and responsibilities of these two organizations are mutually supporting and complementary, and that resources appropriated for a particular purpose are not otherwise spent.

Development of Cyber Capabilities

CYBERCOM has depended heavily to date on NSA for technology, equipment, capabilities, concepts of operations, and tactics, techniques, and procedures.

36. In your view, is DOD properly organized and resourced to provide a broad base of innovation and capability development in the cyber domain? Please explain your answer.

I believe the Department of Defense is properly organized and resourced to enable effective capability development in cyberspace. U.S. Cyber Command's acquisition authorities, its recently-executed enhanced budget control authority, and its eventual Program Executive Office for the Joint Cyber Warfighting Architecture are three critical, Congressionally authorized tools that empower this capability development. In addition, U.S. Cyber Command is maturing its partnerships with other development organizations like the Strategic Capabilities Office and the Defense Advanced Research Projects Agency. The creation of the ASD(CP) role enables greater advocacy in the Department of Defense's resource allocation processes for innovative development opportunities to be available for U.S. Cyber Command. If confirmed, I look forward to working with the Commander of U.S. Cyber Command to understand and close capability development gaps perspective that could help deliver more combat power to defend our nation.

37. As CYBERCOM looks at adapting its cyber force structure as part of CYBERCOM 2.0, how do you think that should or will affect major capability development efforts, such as the Joint Cyber Warfighting Architecture?

Any force structure adaptation should consider updated ways to more rapidly develop and deliver innovative capabilities to our cyber forces. The FY 2023 NDAA directed the establishment of a Program Executive Office, which, combined with previously-granted acquisition authorities, should provide U.S. Cyber Command with the necessary structure and agility to implement whatever changes CYBERCOM 2.0 generates, including integrating outside acquisitions into the Joint Cyber Warfighting Architecture. If confirmed, I look forward to working with U.S. Cyber Command and the services to advance the CYBERCOM 2.0 initiative.

38. How will you advocate for resources in the military services for the science and technology funding for cyber research that will help develop needed future capabilities?

The ASD(CP) is responsible for the DoD's cyber strategy and implementation plan, which directs the Department's proactive approach to defending forward, as well as where the Department needs to make investments to deepen the integration of cyber into our warfighting capabilities. If confirmed, I will work with the Military Department Principal Cyber Advisors and other leaders to identify and support areas where service-sponsored S&T funding adds a competitive advantage for the Department of Defense's cyber posture. I would partner with the Under Secretary of Defense for Research and Engineering to contribute to Department-wide guidance on S&T priorities.

Organization and Management of the Cyber Mission

Congress consciously modeled the organization, management, and oversight of CYBERCOM on the model that has successfully been applied to SOCOM. However, using this model, DOD has not yet overcome persistent and concerning readiness problems in the Cyber Mission Forces – readiness problems that are due to chronically insufficient numbers of high-caliber operators in critical work roles. These shortcomings have become the main argument advanced by advocates of creating a Cyber Force.

39. Do you believe that the SOCOM organizational and management model as applied to the cyber mission is the most appropriate for the Department, or should it be abandoned in favor of starting over with a separate cyber service?

I understand that the Department of Defense is currently evaluating alternatives to generate cyber forces in ways that will address these readiness concerns. While I do not wish to preempt that analysis, I believe a range of options should be considered, including extending aspects of the U.S. Special Operations Command model to U.S. Cyber Command. I believe the goal should be to decide on an approach that will generate the kind of combat power and sustained readiness that will prioritize excellence and mastery in the force. If confirmed, I would look forward to contributing to the decision-making process about new approaches to cyber force generation, and to work with the Congress in so doing.

40. Do you believe that DOD, using the SOCOM model, can and will solve in a timely manner the personnel-related readiness problems that confront the Cyber Mission Force?

I believe DoD can utilize section 1535 of the FY 2024 National Defense Authorization Act to standardize many of the enabling issues that contribute to readiness across the services. For example, there are opportunities to standardize pay for certain roles across the services. I understand that the Department is presently undertaking the work required by section 1535, and if confirmed, I will make it a top priority to synchronize this effort with whatever results may come from the CYBERCOM 2.0 effort.

41. In your view, should the Department and Congress provide CYBERCOM with additional personnel management authorities in order to solve these readiness problems?

Congress has been very supportive of flexible authorities for cyber personnel management at the Department of Defense. For example, the authority for a Cyber Excepted Service created new avenues to recruit and retain civilian talent that can complement uniformed talent in critical operational roles. If confirmed, I will review the totality of personnel management authorities available to U.S. Cyber Command and determine if additional authority would make a material difference. If so, I will communicate that determination to the Secretary and to Congress.

42. How will you work with others in DOD and the interagency, including the DOD CIO, the Undersecretary of Defense for Personnel and Readiness and the Office of Personnel Management, to identify and coordinate any requests for new personnel management authorities?

If confirmed, I will work across the Department of Defense to ensure that cyber forces are receiving the talent, equipment, resources, and authorities needed to compete and win in cyberspace. I will partner with the DoD Chief Information Officer (DoD CIO) and Under Secretary of Defense for Personnel and Readiness (USD(P&R)) through the Cyber Workforce Management Board to ensure personnel policies appropriately support force development for uniform members and civilians. I will partner with the Commander of U.S. Cyber Command to ensure that it institutionalizes the force development processes required for its future talent and force design needs. I will advocate for those requirements within the Office of the Secretary of Defense and to the services.

Personnel Readiness in the Cyber Mission Force

The 2023 Military Cyber Strategy stated "The Department will prioritize reforms to our cyber workforce and improve the retention and utilization of our cyber operators. In so doing, we will assess diverse alternatives for sizing, structuring, organizing and training the Cyberspace Operations Forces and their relationship to Service-retained cyber forces."

43. What steps have the services taken so far to achieve necessary high levels of personnel readiness in the Cyber Mission Force (CMF)?

I understand the Department of Defense is exploring a range of options to maximize the readiness of its cyber forces to meet their assigned missions and maintain operational advantage over our adversaries. From my experience with the Army, we have good examples of how service-retained elements can complement the Cyber Mission Force while also pursuing priorities for Army commanders. If confirmed, I look forward to understanding how the other services manage their service-retained cyber forces and to ensuring that these efforts support the best defense of the nation in cyberspace.

44. What policies or processes do you anticipate implementing to try to get better insight into tracking and remediating the issues related to service personnel readiness for the CMF?

If confirmed, I would begin with policies and processes highlighted in section 1535 of the FY2024 National Defense Authorization Act that, if standardized, can lead to improved service personnel readiness. I understand that the services often use different tracking databases and so using existing tools to gain Department of Defense-wide insights will be a key priority. If confirmed, I will work with U.S. Cyber Command and the services to refine the policies and processes for improving readiness within the Cyber Mission Force.

Intelligence Support for Challenging Cyber Targeting Requirements

The National Defense Authorization Act for Fiscal Year 2024 also noted that improved intelligence support is critical for the success of cyber operations conducted in support of Combatant Command Operational Plans in conflict, which depend on non-kinetic means to neutralize critical adversary assets. This specialized intelligence support would complement and extend the work of the task force for Counter-Communications, Command, Control, Computing, Cyber and Intelligence Surveillance and Targeting (C5ISRT).

45. What is your understanding of this requirement and challenge?

The Department of Defense relies on timely and actionable intelligence to support cyber operations against increasingly capable adversaries. The Department recognized this requirement in the 2023 DoD Cyber Strategy and is prioritizing improved intelligence support to meet the needs of the cyber operations community. I understand that U.S. Cyber Command and the Defense Intelligence Agency are exploring a pilot effort to improve foundational cyber intelligence, as General Haugh testified before the Senate Armed Services Committee earlier this year. If confirmed, I will work to understand the status of this pilot. I will also work with my colleagues in the Office of the Under Secretary of Defense for Intelligence and Security to ensure the needs of the cyber warfighter are prioritized.

46. If confirmed, how would you persuade the leadership of the Department, the Director of National Intelligence, the Under Secretary of Defense for Intelligence and Security, and the heads of appropriate DOD components of the Intelligence Community, especially the National Security Agency, to deliver this support?

If confirmed, I will need to more concretely familiarize myself with current impacts of intelligence gaps to the joint force and the requirements from operational commanders. Depending on the nature of those gaps, I would evaluate on-going efforts such as the DIA-U.S. Cyber Command pilot. I would also examine what steps are available under present authorities to improve the provision of this support, such as enhanced information sharing and human capital development. Ultimately, I would build a coalition with the Commander of U.S. Cyber Command, the Under Secretary of Defense for Intelligence and Security, and others to generate a way forward that will promote the best defense of the nation.

47. In your view, will it be necessary to establish an organization to ensure that this requirement is fulfilled on a sustained basis?

If confirmed, I will consider all options to ensure our cyber operators receive the necessary intelligence support to perform their missions. I understand the Department of Defense has engaged Congress on the means to address intelligence gaps and the unique requirements of cyber operations to achieve meaningful effects in cyberspace. I look forward to further exploring the work that has been done on this issue and engaging with Congress on the best means to deliver support to the cyber warfighter.

Data Support for Intelligence Analysis and Operational Support for the Cyber Mission

Section 1523 of the National Defense Authorization Act for Fiscal Year 2024 tasked the Chief Digital and Artificial Intelligence Officer (CDAO) with providing the digital infrastructure and procurement vehicles and responsible executive agents necessary to acquire and manage data assets and data analytics capabilities at scale to enable an understanding of foreign key terrain and relational frameworks in cyberspace to support the planning of cyber operations, the generation of indications and warnings regarding military operations and capabilities, and the calibration of actions and reactions in strategic competition. This mandate is necessary because DOD has never developed a data strategy to gather, analyze, and apply the immense digital data available about activities taking place in key foreign regions.

48. **What role do you foresee playing in influencing policy and resource allocation in the Department to fulfill this mandate in support of the cyber and related information operations missions that you will oversee, if confirmed?**

    The Chief Digital and Artificial Intelligence Officer (CDAO) is DoD's senior official responsible for the acceleration and adoption of data, analytics, and artificial intelligence (AI) to generate decision advantage. If confirmed, I look forward to supporting CDAO's efforts to ensure the provisions of section 1523 are carried out in line with the 2023 DoD Data, Analytics, and AI Adoption Strategy.

49. **What is your understanding of the foundational benefits to the cyber mission of data on foreign Internet connections, routing of Internet traffic, and mapping of cyber terrain?**

    A dynamic understanding of the systems, protocols, data, software, processes, cyber personas, and networked entities that comprise and control cyberspace is essential to support DoD's cyber operations planning. If confirmed, I look forward to working with CDAO and other DoD components to advance the Department's foundational understanding of the shared digital operating environment and protect our cyber infrastructure.

Integrated Non-Kinetic Force Development

Section 1510 of the National Defense Authorization Act for Fiscal Year 2023 mandated that the Secretary of Defense establish a force planning activity through the Under Secretary of Defense for Research and Engineering to identify and define the relevant forces, capabilities, and information support required to develop and deliver non-kinetic effects within a defense planning scenario. This requirement was prompted by the fact that the Department is undertaking the development of technical capabilities to conduct effective non-kinetic operations, but had no plans to develop the forces and command and control processes and relationships necessary to make use of such capabilities.

50. What is your level of understanding of this statutory requirement and how it relates to the cyber mission of the Department?

I understand the USD(R&E) is organizing the Non-Kinetics Force Planning Activity and that this work is ongoing. I would anticipate that cyber forces and capabilities will play a role in this force planning activity. If confirmed, I am committed to fully supporting this analysis and expect the ASD(CP) to have an active role in the plan's execution.

51. What role do you intend to play in helping to execute this force planning requirement?

The Department of Defense must be able to deliver integrated non-kinetic effects, including through the electromagnetic spectrum and in cyberspace. If confirmed, I will fully support this force planning activity and expect the ASD(CP) to have an active role in the plan's execution.

Provision of Acquisition Expertise to CYBERCOM

Congress and the Secretary of Defense have provided to the Commander of CYBERCOM the authority to control the expenditure of funds for the acquisition of foundational capabilities to operate in cyberspace, and to manage the programs that are to provide such capabilities. However, successful management of the development of technically complex cyber capabilities will require personnel who have expertise in systems acquisition and the relevant technology. Congress has therefore stressed the need for the leadership in the Department to assist CYBERCOM in acquiring this expertise.

52. If confirmed, you would be responsible for service secretary-like functions with respect to the cyber mission. How do you intend to assist CYBERCOM in acquiring crucial systems acquisition expertise?

The Department of Defense's work to recruit, retain, and produce top acquisition talent will be an on-going priority given the competition with industry for these sought-after skillsets. There is a recognized shortage of skilled cyber acquisition personnel within the Department that goes beyond compensation and incentives and is connected to complete career progression. If confirmed, I am committed to working with the USD(P&R), USD(A&S), Defense Acquisition University, and the DoD CIO on efforts like the FY 2023 NDAA section 835 for Software and Cybersecurity Acquisition curriculum updates and the DoD Cyber Workforce Strategy that seek to leverage talent exchanges and career broadening opportunities, cultivate talent pipelines within the Defense Acquisition Workforce and Cyber Excepted Service (CES), and enhance cross-training and information sharing to harmonize our efforts across the Department of Defense.

2023 DOD Cyber Strategy

53. DOD published its updated Cyber Strategy in 2023. In your opinion, what are the key changes in the new strategy and what are the main elements of continuity?

The 2023 DoD Cyber Strategy places an emphasis on working with allies and partners in cyberspace, identifies force generation and intelligence reforms as critical to building enduring advantages in cyberspace, and highlights key investment areas to deepen integration of cyber into warfighting capabilities. In terms of continuity, this fourth iteration of the Defense Cyber Strategy builds upon and supports the Department of Defense's proactive approach to defending forward and persistent engagement.

54. What do you see as the primary cyber policy challenges facing the defense industrial base, and, if confirmed, what suggestions do you have for addressing them?

The Defense Industrial Base (DIB) plays an important role in developing, manufacturing, and maintaining technologies vital to national defense. The DIB faces persistent threats from malicious cyber actors, which not only impose significant opportunity costs by diverting resources from core missions but also complicate Department of Defense acquisition processes, ultimately increasing costs for taxpayers. To enhance DIB cybersecurity, the Department must leverage public-private partnerships for rapid detection, response, and recovery of critical DIB assets and ensuring the reliability of essential production nodes. I would highlight the work of the National Security Agency's Cybersecurity Collaboration Center as a model of how the government can empower and learn from industry partners to promote improved cybersecurity. If confirmed, I would work closely with contract and procurement officials to understand what incentives and reinforcements are available to promote improved cybersecurity.

55. In your view, how do you think artificial intelligence can be leveraged in the implementation of DoD's Cyber Strategy?

The 2023 DoD Cyber Strategy builds upon and supports the Department of Defense's proactive approach to defending forward, including identifying where DoD needs to make investments to deepen the integration of cyber into our warfighting capabilities. When applied to cyber missions, artificial intelligence has the potential to improve vulnerability research and access development and accelerate the speed and scale of many aspects of conducting cyber operations. AI also has the potential to enable our adversaries and competitors, and so must be viewed through an intelligence and protection perspective as well. If confirmed, I look forward to working with the DoD Chief Information Officer and Chief Digital and Artificial Intelligence Office to ensure that we use AI in a responsible and effective way to advance the objectives of the 2023 DoD Cyber Strategy.

Election Security

CYBERCOM and NSA, under dual hat management, have partnered since the 2016 presidential election to protect elections from foreign interference. Former Commander of CYBERCOM and Director of NSA, General Nakasone, consistently referred to election security as a "can't fail" mission of these two organizations.

56. Do you agree that protecting elections against foreign interference is a critical mission of CYBERCOM and NSA? Do you intend to make that clear if you are confirmed?

Yes, defending U.S. elections against foreign interference is a critical mission for the Department of Defense. I understand that DoD supports the whole-of-government effort to ensure the security and integrity of U.S. elections by focusing on stopping malicious foreign cyber activity at its source and providing technical support to domestic partners when requested and authorized.

57. Can you provide any unclassified highlights for what kinds of support CYBERCOM has provided for election security since 2016?

I understand that the 2024 U.S. Presidential elections will mark the fourth time that the joint NSA and U.S. Cyber Command Election Security Group has supported the whole-of-government effort to defend U.S. elections against foreign interference. Ahead of the 2020 U.S. election, the government of Montenegro invited a U.S. Cyber Command hunt forward team to discover new malware and understand how to improve defenses from it. If confirmed, I will work closely with U.S. Cyber Command and the National Security Agency to support the whole-of-government effort, including generating insights gained through hunt forward activities like those in Montenegro, to defend the 2024 election from foreign interference.

58. In what ways has CYBERCOM support for election security implemented or reinforced training and certification requirements within its workforce to ensure any activities supporting election security protect U.S. citizen privacy and civil liberties?

U.S. Cyber Command is part of a whole of government effort, partnered with DHS, FBI, and other federal agencies, to defend U.S. elections from foreign interference. DoD's effort is led by the Election Security Group, a joint U.S. Cyber Command-NSA Task Force under the command of General Haugh. The Election Security Group is focused on generating insights on foreign adversaries, enabling better defenses by working with U.S. agencies, allies, and partners, and imposing costs on foreign adversaries if they attempt to interfere in our elections. U.S. Cyber Command operations focus on foreign actors operating outside the United States. U.S. Cyber Command personnel are trained on intelligence community standard intelligence oversight procedures to ensure the rights of U.S. citizens are protected. I understand that compliance requirements, as well as the privacy and civil liberties training that is required of DoD personnel, are routinely

evaluated by Inspectors General across the force. If confirmed, I will support this no-fail mission to protect our elections from foreign interference and the work of the Election Security Group of targeting foreign actors abroad, while protecting the rights and privacy of U.S. citizens.

Red Team Modernization

Cyber Red Teams play a critical role in DOD's cybersecurity mission. However, there is no overarching management entity ensuring consistency in the capabilities of all the Red Teams that exist in DOD components. The Director of Operational Test and Evaluation, which makes extensive use of Red Teams, has informally stepped up to advocate for the Department's Red Teams, including their modernization. Congress mandated in section 1660 of the National Defense Authorization Act for Fiscal Year 2020 that DOD perform a joint assessment of Red Team needs, and section 1507 of the National Defense Authorization Act for Fiscal Year 2024 required that another joint review assess the status of the implementation of the recommendations from the first one.

The Principal Cyber Advisor to the Secretary of Defense is among the officials named in these sections. In your position as Principal Cyber Advisor to the Secretary and Chief of Staff on the Army, you were responsible for oversight of the Army's cyber Red Teams.

59. What priority do you assign to the modernization of the capabilities of DOD Cyber Red Teams?

I assign a high priority to the modernization of DoD Cyber Red Teams because they sharpen our cyber defenses and defenders to stay ahead of evolving threats. As Principal Cyber Advisor for the Army, I see the value that the red teams from the Threat Systems Management Office, Army Cyber Command, and the Corps of Engineers bring to improving our defenses. The DoD CIO released Department of Defense Instruction 8585.01 earlier this year, which established policies and assigned responsibilities for all Cyber Assessment Programs to include the DoD Cyber Red Teams. If confirmed, I look forward to working with the DoD CIO, U.S. Cyber Command, and the DoD Cyber Red Team community to ensure we continue to modernize the capabilities our assessment teams employ.

60. What approach will you take, if confirmed, to advocate for the health and capacity of Red Teams?

If confirmed, I will advocate for the health and capacity of Cyber Red Teams by incorporating resourcing of these teams into my budget certification responsibilities, as they are critical enablers of cyber operations. I will work with the Principal Cyber Advisors of the Military Departments to understand their plans for these teams, and I will work with the DoD CIO on the implementation of Department of Defense Instruction 8585.01 to enable additional support for Cyber Red Teams.

Cybersecurity of the Nuclear Command, Control, and Communications Network

Congress has consistently expressed concern in successive NDAAs about the state of the cybersecurity of the Nuclear Command, Control, and Communications (NC3) and has specifically required a Strategic Cybersecurity Program to ensure the security of the most critical DOD missions, among which is nuclear deterrence.

61. What are your views about the priority of securing the NC3 network and the severity of current security shortfalls?

Ensuring the cybersecurity of our nuclear command, control, and communications (NC3) systems is an essential mission for the Department of Defense. I am committed to assessing and identifying potential cyber vulnerabilities to U.S. NC3 systems, and if any exist, remediating them as called for in successive Congressional requirements including FY 2021 section 1712 and 1714 and FY 2022 section 1525, 1534, and 1644. If confirmed, I will review the Department's work under these NDAA sections and offer recommendations to the Secretary if there are additional areas that require focus.

62. If confirmed, what role do you envision in supporting the work of the NC3 cross functional team?

Section 1512 of the FY 2024 NDAA directs the Secretary of Defense to establish a cross-functional team to develop and oversee the implementation of a threat-driven cyber defense construct for the networks that enable NC3. If confirmed, I look forward to supporting this important work alongside my OSD colleagues and in coordination with each of the military departments, the Defense Information Systems Agency (DISA), the National Security Agency (NSA), U.S. Cyber Command, and U.S. Strategic Command

Deterrence of Cyber Attacks on US Critical Infrastructure

The 2023 Military Cyber Strategy and testimony from multiple administration witnesses affirm that the Peoples Republic of China (PRC) will 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 tangible confirmation of these forecasts.

63. In your view, is it a violation of the law of armed conflict for the PRC or other adversaries to disable CI if that infrastructure is providing essential support to military capabilities and operations?

As with malign activity in any other domain, Department of Defense leaders, in coordination with the Intelligence Community, the State Department, and other key Executive Branch partners, assess and advise the President whether malicious cyber activities alone or in concert with other acts constitute a violation of the law of armed

conflict. I understand that malicious cyber activities that do not constitute a use of force may nonetheless cause strategic effects, constitute violations of other international legal rules or international norms, or warrant appropriate responses.

64. Based on current understanding of PRC intentions, does it appear likely that the PRC be deterred from conducting cyber attacks against CI located in the U.S. homeland in a conflict if we are not prepared to respond in kind?

In my view, the PRC continues to make investments in a broad range of cyber capabilities, including those that enable the targeting of U.S. critical infrastructure and supporting networks. Both critical infrastructure and essential warfighting networks contribute to a timely and effective response from the U.S. military, including our cyber operations forces. While the PRC likely perceives a high-cost imposition for conducting a cyber attack on critical infrastructure during peacetime, the PRC's prepositioning efforts indicate they remain interested in these as potential options during conflict.

If confirmed, I will prioritize ongoing efforts across the Department of Defense that strengthen relationships with private providers and fortify cyber defense across the nation's critical infrastructure. I will also work closely with the Commander of U.S. Cyber Command to ensure a range of options is available for responding to an attack against U.S. critical infrastructure.

65. What practical considerations or constraints might impede the development of capabilities and plans to respond in kind to PRC threats and preparations to attack US-based CI?

The cross-government effort to disrupt and respond to PRC threats against U.S. critical infrastructure would be my highest priority, if confirmed. In my view, Department of Defense efforts to generate a skilled, trained, and experienced cyber workforce (uniformed and civilian, active, guard, and reserve) is a critical consideration and enabler to defending the nation from these threats. The Department also faces a complex authorities landscape with private providers while other federal agencies often take leading roles in the provision and protection of infrastructure. If confirmed, I will work with the Commander of U.S. Cyber Command, partners across the interagency, and private sector stakeholders to ensure we can coordinate to prevent and respond to such threats.

66. How would you recommend that the U.S. Government respond to the revelations about the PRC's Volt Typhoon operations, or such similar operations in the future?

In my view, there are a number of whole-of-government initiatives that contribute to enhancing U.S. cybersecurity outcomes aimed at identifying and ultimately mitigating threats as described in recent reports about Volt Typhoon. If confirmed, I would continue to champion the public cybersecurity advisories published by the NSA, CISA, DOE, and other U.S. departments and agencies, as well as those published with our foreign partners.

These advisories, both technical and qualitative, offer one source of information for operators and defenders to hunt their own networks for adversary activity, expel potential intrusions, and ultimately harden these critical networks against PRC activities. I would also support efforts to improve the resiliency of this infrastructure, technical measures to accelerate the detection and expulsion of threats, and the generation of options for a campaign to counter these activities.

67. In your view, does DOD have a role in supporting civilian CI in the event of a major cyber event?

While the DoD is the Sector Risk Management Agency (SRMA) for the Defense Industrial Base (DIB), other departments and agencies serve as such for energy, information technology, and other sectors. These departments and agencies lead Federal risk management efforts for each of the sixteen designated critical infrastructure sectors. In my view, the Department of Defense has an opportunity to partner with the other SRMAs across critical infrastructure sectors, to generate and share insights on foreign malicious cyber threats, and to offer best practices for effective remediation to enable better defense. If confirmed, I will make it a priority to support requests for assistance from federal civilian agencies or the private sector through appropriate channels.

68. What policy processes or authorities come into play for DOD to more actively work with DHS or the CI providers in such a situation?

I understand that DoD cyber forces and personnel can provide support to DHS or another Federal Agency under a Defense Support to Civil Authorities request in response to a crisis or natural disaster, or in support of special events, when Federal, State, local, tribal, and territorial capabilities are overwhelmed, exhausted, or when DoD has military-unique capabilities that are needed. I am also aware of the FY 2024 NDAA-directed update to Executive Order 12304, which granted new authority to the Secretary to activate Reserve Component personnel for significant cyber incidents. If confirmed, I look forward to working with DHS and other federal agencies to ensure the Department of Defense is postured to support such requests.

Software Bills of Materials

Among the best practices in cybersecurity is to require providers of information technology to supply a software bill of materials (SBOM) showing the provenance of all the software components in the products they provide. SBOMs provide the ability to identify where discovered software vulnerabilities reside in the enterprise for patching purposes and to screen for risky code.

69. Do you consider decisions about adopting requirements such as SBOMs to be solely up to the Chief Information Officers of DOD components and the Secretary and Deputy Secretary of Defense, or should the Principal Cyber Advisor (PCA) and the PCAs of the military services be involved in such decisions?

The DoD Chief Information Officer is the principal staff assistant and senior advisor to the Secretary of Defense and Deputy Secretary of Defense for all matters relating to the DoD information enterprise including cybersecurity, communications, and information systems. If confirmed, I would very much involve myself with these kinds of decisions that have the potential to improve the Defense Department's cybersecurity. I would also involve the Principal Cyber Advisors of the Military Departments to ensure they can partner with service Chief Information Officers on cybersecurity issues like a Software Bill of Materials (SBOMs).

70. What are your views about adoption of a policy of requiring SBOMs?

Because of its modular nature, software is often dependent on sub-components that may introduce inadvertent risks. In my view, SBOMs can give program managers and cybersecurity personnel much-needed insight into the software supply-chain of critical applications. While I am supportive of initiatives like SBOMs, they must be implemented in a secure way so that the information they contain is not exploited. The 2023 Department of Defense Software Modernization Implementation Plan calls for establishing SBOM Implementation Guidance for DoD. If confirmed, I look forward to working with the DoD CIO and other components to ensure the Department operates with a secure software supply chain.

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.

71. If confirmed, what actions would you take were you to receive or become aware of a complaint of sexual harassment or discrimination from an employee of the Office of the ASD(CP)?

I am committed to addressing any instance of sexual harassment and gender discrimination. First, I would familiarize myself with the appropriate reporting channels and procedures in the Office of the Secretary of Defense. Second, I would ensure that those working in the Office of the ASD(CP) are also aware of the most current requirements and procedures for how to prevent, and if necessary, respond to such situations. I will follow the appropriate Departmental protocol with DoD leadership to address any such matter.

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.

72. 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.

73. 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.

74. 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.

75. Do you agree, without qualification, if confirmed, to keep this committee, its subcommittees, other appropriate committees of Congress, and their respective staffs apprised of new information that materially impacts the accuracy of testimony, briefings, reports, records—including documents and electronic communications, and other information you or your organization previously provided? Please answer with a simple yes or no.

Yes.

76. 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.

77. 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.

78. 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.