Senate Armed Services Committee
Advance Policy Questions for Katherine Sutton
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." If confirmed, you will be the second person to officially serve in this position.

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

As stated in 10 U.S. C. § 138, the principal duty of the Assistant Secretary of Defense for Cyber Policy is "overall supervision of policy of the Department of Defense for cyber." I understand this to include ensuring alignment of DoD cyber policy with national cyber policy and developing, implementing, and integrating DoD cyber policy across the Department in support of the Under Secretary of Defense for Policy and the Deputy and Secretary of Defense. Concurrently, the ASD(CP) serves as the Secretary of Defense's Principal Cyber Advisor (PCA), providing expert counsel on military cyber forces and activities. In this capacity, the PCA oversees the responsibilities given to Commander (CDR), U.S. Cyber Command (USCYBERCOM) under 10 U.S.C. § 167b, in particular with regard to the organization and readiness of cyber operations forces assigned to USCYBERCOM. The PCA also certifies the sufficiency of the Department's cyber budget and provides input to the Planning, Programming, Budgeting, and Execution (PPBE) process related to cyber forces and capabilities.

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

If confirmed, I anticipate the Under Secretary of Defense for Policy will look to me to assist the Secretary of Defense in enacting the President's priority of restoring peace through strength in the cyber domain. I intend to do this by focusing on the Secretary's objectives of defending the homeland, deterring China, and increasing burden sharing with allies and partners through cyber.

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

I believe my diverse background in engineering, policy, and strategic leadership qualifies me to serve as the Assistant Secretary of Defense for Cyber Policy. With over two decades of service advancing our national security across the cyber domain and emerging technologies, I have consistently delivered results through both technical execution and policy development. My work has spanned cybersecurity, space systems, nuclear

nonproliferation, and emerging technologies like 5G, synthetic biology, quantum computing, and artificial intelligence—each contributing to a deep, mission-driven understanding of the evolving cyber landscape and the critical need for innovation in defense capabilities.

I hold a Bachelor of Science from the University of Illinois at Urbana-Champaign and a Master of Science from Stanford University, both in electrical engineering, which have provided me with a deep foundational understanding of cyber and emerging technologies. During my 15 years at Sandia National Laboratories, I served in a variety of technical and leadership roles across high-impact national security programs in nuclear weapons, space, and cyber, successfully leading programs responsible for critical national security systems, managing teams, and advising on key research and development (R&D) programs. I led cross-functional teams delivering secure space-based systems, managed a cybersecurity R&D department supporting various government customers, designed components for nuclear weapons use control, and ran an electromagnetic test lab. These roles honed my ability to lead multidisciplinary teams, manage complex government programs, and integrate strategic planning with technical innovation.

My experience with defense policy and the legislative process in Congress has given me a robust understanding of the national defense landscape. As a professional staff member focused on cybersecurity and emerging technology, I developed the skills to engage with stakeholders and lead coordinated policy initiatives at the national level. In my current role as the Cyber Command chief technology advisor, I have gained valuable insights into the strategic and operational aspects of the Command's missions, overseeing and synchronizing efforts across the Command and Department. This range of experiences has prepared me well to execute the responsibilities of the Assistant Secretary of Defense for Cyber Policy.

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?

Throughout my career, I have had opportunities to lead diverse, multidisciplinary teams across both the government and Sandia National Laboratories, experiences that have prepared me well to serve as Assistant Secretary of Defense for Cyber Policy.

At Sandia, I held several key leadership and management roles that developed a broad set of skills. As a research and development manager, I oversaw a department of engineers responsible for cybersecurity programs supporting agencies such as the Department of Energy and the Department of Homeland Security. I managed day-to-day staff performance, project execution, customer engagement, strategic planning, and capability development, while also mentoring team members. As project lead for the Global Burst Detector system, I directed a high-performing team, successfully delivering a complex next-generation nuclear detonation detection system. Additionally, as technical lead for an RF telemetry space payload, I guided a multi-disciplinary engineering team through

the full development lifecycle, driving system architecture, design, and integration to meet critical mission requirements.

In government, I have led major strategic initiatives and shaped key defense policy efforts. At U.S. Cyber Command, I was responsible for leadership of a key strategic initiative. My responsibilities included managing senior-level engagements, facilitating Department collaboration, and aligning initiatives with policy and budget priorities. While serving on the House and Senate Armed Services Committees, I was the professional staff lead for a broad portfolio spanning cyber, 5G, AI, and emerging technologies. I was the staff lead for legislative initiatives that resulted in significant reforms, including provisions that implemented key recommendations from the Cyberspace Solarium Commission and strengthened cyber operations and innovation. I also mentored junior staff, coordinated legislative activities across chambers, and supported committees across the Senate in developing effective policy. Across all these roles, my leadership has consistently focused on building cross-functional teams, driving mission-aligned outcomes, and advancing national security priorities through both technical and policy expertise.

Major Challenges and Priorities

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

In my view, China poses the most significant cyber threat to the Department and to the nation in cyberspace. China has developed sophisticated cyber capabilities and deploys them at scale to exploit vulnerabilities in U.S. critical infrastructure, conduct espionage, and challenge our military advantages. Russia, Iran, and the Democratic People's Republic of Korea (DPRK), as well as cyber criminals and violent extremist organizations, conduct malicious cyber activities that further threaten the homeland and challenge our deterrent posture.

To achieve the President's vision of peace through strength, the Department must address these threats through day-to-day competition in the cyber domain while remaining postured to fight and win in a contested cyber environment. If confirmed, I will work to develop our cyber capabilities and ensure they're integrated with other non-kinetic capabilities in support of warfighting requirements.

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

If confirmed, I would focus on reinforcing American dominance in the cyber domain to enhance the lethality of the Joint Force, reestablishing deterrence, and defending the homeland against cyber threats. I would work to ensure that U.S. Cyber Command possesses the authorities and resources it needs to deter and defeat cyber threats to our nation. I would also work to fully integrate our defense cyber capabilities into a whole-of-government approach, combining kinetic and non-kinetic capabilities and using all

tools of national power to combat adversary cyber threats. Finally, I would ensure the Department leads in identifying, developing, procuring, and integrating cutting edge technologies in a fast and efficient manner to reinforce our warfighting advantages.

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

I believe it is critical for DoD to have robust, effective, and second-to-none offensive and defensive cyber forces and capabilities to address the top priorities of the President and the Secretary. To meet the President's vision of restoring peace through strength, I would prioritize ensuring that the Department's strategies, plans, and capabilities for the cyber domain are tailored to the unique threats we face and provide maximum options to the President and to the Secretary. These options should be designed to reinforce deterrence and, if necessary, reinforce our military advantages in wartime. I would further look forward to working closely with the Commander of U.S. Cyber Command, to ensure the Command is successful in executing its service-like authorities, including the enhanced budget authorities recently granted to U.S. Cyber Command by Congress.

The Department has struggled to be timely in responding to the statutorily mandated congressional reporting requirements related to cyber, often being several years behind in responding to some requirements.

8. How do you propose to address this backlog, and prevent it from happening again in the future?

It is my understanding that, especially since last year's focused conversations between the Department and Congress on this issue, clearing the backlog of overdue congressional reporting requirements has received concerted effort from among Cyber mission elements across the Department. The latest information on this effort forecasts that most, if not all, highest-priority items will be completed and remitted by early summer. If I am confirmed, I will make it a continuing priority to carry this work to completion and substantively eliminate the requirements backlog.

Looking forward, I believe that measures that can prevent this backlog from occurring again are predicated on clear communication between Congress and the Department, as well as intra-departmentally, not only on the substance of requirements, but also on the most appropriate assignment and feasible timeframes for their execution. Additional lag prevention efforts can also help, such as active oversight of cross-department cyber and cyber-related tasks from the OSD level, and closer synchronization with legislative affairs, including making more effective use of enhanced program of record data at the mission-level. I understand that these efforts have already been put in motion.

<u>Civilian Control of the Military</u>

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.

9. 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, Congress created the position of the ASD Cyber Policy because the United States faces one of the most dangerous strategic environments in our Nation's history, requiring the singular focus of a senior civilian leader on DoD cyber matters. Combined with the 10 U.S.C. § 392a authorities vested in the Principal Cyber Advisor to the Secretary of Defense, I believe Congressional intent for this official is to exercise proper oversight and responsibility for cyber strategy, policy, operations, forces, and budgets in support of the Secretary of Defense.

If confirmed, I would exercise service-like authorities over USCYBERCOM as prescribed in 10 U.S.C. § 167b and directed by the Secretary of Defense. I will foster collaboration within the Department and with other departments and agencies to advance the nation's strategic goals. This includes ensuring unity of effort among stakeholders in the Department engaged in offensive and defensive cyber operations and cyber security, along with providing rigorous oversight of cyber forces, budgets, and operations. My focus will remain steadfastly on warfighter support and mission accomplishment.

I am also committed to maintaining a collaborative relationship with Congress and ensuring timely and responsive communication on cyber matters.

10. 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?

My commitment to the principle of civilian control of the military, enshrined in the U.S. Constitution, will be the bedrock of my service as ASD(CP), if confirmed. This commitment will manifest in several concrete actions:

My focus will be on aligning military cyber activities with the broader national security and national defense strategy and policy objectives set forth by the President and the Secretary of Defense. This means prioritizing the development and implementation of cyber capabilities that support these objectives and ensuring that military operations in cyberspace remain firmly within the bounds of established policy and law.

I will provide candid and comprehensive assessments of cyber threats, capabilities, and strategic options to the Under Secretary of Defense for Policy and the Secretary of Defense, including proactively identifying potential areas of friction between military operations and policy objectives and offering solutions that uphold civilian authority.

I will ensure a clear understanding of the respective roles and responsibilities of civilian leadership and military commanders in the cyber domain. This includes emphasizing the civilian authority in setting strategic objectives and priorities, while empowering military commanders to develop and execute operational plans within those parameters. I will work to maintain clear protocols for decision-making, ensuring civilian oversight of cyber operations.

Finally, I will advocate for the development and recruitment of civilian cyber expertise within the Department of Defense. A robust civilian cadre is essential for providing effective oversight and ensuring that military cyber operations are informed by a broad range of perspectives and expertise.

Cyber Policy and Authorities

11. 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?

The President and Secretary of Defense have been clear: China is the primary threat to our national interests and the most significant threat we face in cyberspace. At the same time, we must also manage the cyber threats posed by Russia, Iran, North Korea, and violent extremists and criminal organizations, all of whom continue to invest in a broad arsenal of cyber capabilities, with the clear intention of challenging U.S. national interests at home and abroad. We need to address these challenges while remaining flexible to support the priorities of the President and the Secretary.

Managing these challenges will require continued progression to improve our defenses and deterrent capabilities against longstanding cyber policy challenges, while positioning our still limited cyber resources against the greatest threats. First, we must continue to develop top-tier cyber talent, and I will emphasize speed and agility to ensure our cyber forces outpace those of our adversaries. Our workforce must include specialized talent that can rapidly respond to priorities and develop robust options for the President. Second, we must continuously identify, test, invest in, and adopt cutting-edge private sector technologies. I will also identify any policy challenges to rapidly identifying, experimenting, and adopting capabilities from the private sector that can generate military advantages, including artificial intelligence. Third, we must be prepared to accelerate our operational tempo, consistent with the direction of the President and Secretary. If confirmed, I look forward to overseeing the continued maturation and improvement of U.S. Cyber Command's service-like authorities, while continuing to examine the Department's authorities to ensure our cyber forces move faster than those of our adversaries. Finally, I will deepen our engagement with existing industry partners and explore opportunities to expand these important relationships.

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

a) **The Commander of U.S. Cyber Command:** The Commander of U.S. Cyber Command is responsible for the planning and execution of military cyberspace missions; serving as the cyberspace operations joint force provider and joint force

trainer. Under the direction of the Secretary of Defense and the Under Secretary of Defense for Policy, if confirmed, I would work collaboratively with the CDR USCYBERCOM to ensure the Department has the cyber authorities and resources it needs to advance strategic goals. In addition, 10 U.S.C. 167b(d)(2)(A) assigns CDR USCYBERCOM responsibilities under the authority, direction, and control of the ASD Cyber Policy/Principal Cyber Advisor and I will exercise that authority, direction, and control to the best of my ability.

b) **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 information technology (IT) and spectrum. If confirmed, I will prioritize working closely with the DoD CIO to strengthen our approach to cybersecurity, communications, information systems, supply chain security, and spectrum management. This collaboration is essential given the CIO's critical role advising the Secretary and Deputy Secretary of Defense on these IT issues, and their responsibility as the functional manager for the cyber workforce.

c) **The Military Service Principal Cyber Advisors:** Each Military Department has a Principal Cyber Advisor (PCA) responsible for overseeing and managing that service's cyber posture, including its readiness, capabilities, budget, and strategic direction. As the Principal Cyber Advisor to the Secretary of Defense, if confirmed, I will work closely with the Military Department PCAs to develop and implement DoD-wide cyber policy and strategies.

d) **The Under Secretary of Defense for Intelligence and Security:** The ASD(CP) and USD(I&S) have a critical, intertwined relationship due to the convergence of cyberspace, intelligence, and security. The USD(I&S) provides cyber threat intelligence to inform ASD(CP)'s policy development for defensive and offensive cyber operations, as well as international cyber cooperation. Reciprocally, the ASD(CP) guides the USD(I&S) on intelligence usage and protection. This collaboration is essential for incident response, proactive cyber defense, and aligning cyber operations with national and international law. They also cooperate on international cyber issues like arms control and cybercrime, and coordinate budget allocation for cyber defense initiatives. While the USD(I&S) has a larger budget encompassing all intelligence and security activities, the ASD(CP) advocates for resources dedicated to cyber policy and related programs. This necessitates coordination to ensure proper alignment of Military intelligence Program (MIP) funding to support cyber operations.

e) **The Joint Chiefs of Staff:** The ASD(CP) and Joint Staff have a vital relationship, translating cyber policy into military strategy and operations. ASD(CP) provides policy guidance for integrating cyber capabilities across warfighting domains, ensuring alignment with national security objectives. The ASD(CP) and Joint Staff collaborate on developing cyber doctrine, identifying capability requirements (and improving the JCIDS process to do so more effectively), and informing cyber operations. Jointly, the ASD(CP) and Joint Staff ensure cyber intelligence informs military planning, develop training, and present a unified

DoD position in interagency discussions. This partnership is essential for integrating cyber power into military strategy.

f) **The DOD Chief Digital and Artificial Intelligence Officer:** The Chief Digital and Artificial Intelligence Office (CDAO) leads DoD's efforts to rapidly adopt data, analytics, and AI for improved decision-making in line with the Secretary's focus on innovation, lethality and readiness If confirmed, I will partner with the CDAO and other DoD and OSD offices to integrate these technologies and create a lasting advantage for the Department and the nation.

g) **The Director of the Defense Information Systems Agency:** The ASD(CP) and DISA Director would have a close, collaborative relationship. The ASD(CP) sets cyber policy, while DISA implements it on the DODIN, including security standards, defensive tools, and incident response. They collaborate on capability development, incident response, budget coordination, and ensuring cybersecurity standards are up-to-date. Essentially, the ASD(CP) defines the "what" in cyber policy, and DISA the "how" on the DODIN, ensuring its security and resilience.

h) **The Director for the Defense Advanced Research Projects Agency:** The Defense Advanced Research Projects Agency (DARPA) invests in breakthrough technologies for national security such as the Constellation program, a joint effort with U.S. Cyber Command to rapidly transition cyber capabilities from the lab to the battlefield. If confirmed, I will work with DARPA and U.S. Cyber Command to deliver and operationalize these cutting-edge cyber capabilities and empower warfighters across the full spectrum of operations.

i) **The Director for the Defense Cyber Crime Center:** The Defense Cyber Crime Center (DC3), a designated Federal Cyber Center and DoD Center of Excellence for Digital and Multimedia Forensics, plays an important role in protecting the Defense Industrial Base (DIB) from cyber threats. Along with the Office of the Under Secretary of Defense for Policy (USD(P)), which serves as the DIB's Sector Risk Management Agency, DC3 shares responsibility for safeguarding this critical infrastructure. If confirmed, I will work to ensure the efforts of DC3 and USD(P) are fully synchronized to maximize the protection of the DIB, combating cybercrime, and enhancing cybersecurity.

j) **The Defense Security Cooperation Agency:** DSCA is responsible for the execution and administration of security cooperation programs, as well as the provision of defense articles, training, and other defense-related services. DSCA's role is key in enabling the Department to build the capability and capacity of our allies and partners to help secure networks and sensitive information in cyberspace. If confirmed, I will work with DSCA to ensure the Department's approach to cyberspace security cooperation is fast and flexible enough to advance the President and Secretary's priorities.

k) **The Director of Cybersecurity and Infrastructure Security Agency at DHS:** A strong DoD-DHS partnership is essential for securing America's critical

infrastructure. If confirmed, I will prioritize close collaboration with DHS, enhancing communication and coordination, and seek to ensure DoD is ready to support DHS and other federal civilian agencies where appropriate.

l) **The White House Office of the National Cyber Director:** The National Cyber Director plays a critical role in safeguarding our nation's security and prosperity. As the principal advisor to the President on cybersecurity policy and strategy, the ONCD is essential for coordinating a whole-of-government approach to confronting evolving cyber threats. If confirmed, I will work closely with ONCD to advance the President's cybersecurity objectives.

m) **The Director of the Defense Intelligence Agency:** The Director of the Defense Intelligence Agency (DIA) provides military intelligence to support operations and manages foreign military intelligence for the Nation in addition to other select functions across the greater Intelligence Community. If confirmed, I will work closely with the DIA Director to ensure timely, actionable intelligence for cyber operations and explore the intersection of emerging technologies and cyber capabilities.

Deterrence in cyber space remains a critical principle of national security. The strategy of deterrence through strength is a core element of this administration, and one that, in cyberspace, requires detailed awareness of the domain and robust capabilities.

13. How do you define deterrence in cyberspace? What are the critical elements for a successful deterrence strategy?

Under President Trump and Secretary Hegseth's leadership, I understand that DoD is focused on restoring deterrence across all domains, including cyber. I see deterrence in cyberspace as a combination of denial, resilience, and credible response options. If confirmed, one of my core goals as ASD Cyber Policy will be to ensure the Department has the offensive and defensive capabilities and resources necessary to credibly deter adversaries from targeting the United States and, if necessary, to respond decisively and aggressively. I will work to review the capabilities we have in our toolkit, integrate military cyberspace capabilities with other tools of national power, and restore deterrence in the cyber domain.

14. For deterrence to be credible, adversaries must have some awareness regarding the capabilities they know or suspect we have. On the same token, some strategic ambiguity can also be advantageous for the U.S. How should the Department be thinking about decisions of reveal or conceal when it comes to U.S. cyber capabilities? What role should perception management or even deception capabilities play in those decisions?

Although I am not aware of the full extent of the Department's cyber capabilities and policies, I am committed to ensuring DoD has the cyber capabilities, resources, and policies necessary to enhance the lethality of the Joint Force, reinforce deterrence, and defend the homeland. I wholeheartedly agree that perception management is a critical

component of deterrence. If confirmed, I will review DoD's cyber capabilities and policies and carefully assess the role of cyber in influencing or managing adversary perceptions.

15. In your view, is the current level and tempo of cyber attacks on the Department and on the Nation tolerable?

I believe cyber attacks against the United States are of grave concern, and I would regard it as a critical part of my role, if confirmed, to improve our Nation's defenses and deterrent against them. Deterrence is possible in cyberspace and can be made more effective through a combination of denial, resilience, and credible responses. If confirmed, I will review the capabilities we have in our toolkit, integrate military cyberspace capabilities with other tools of national power, and restore deterrence in the cyber domain. One of my core goals as ASD Cyber Policy will be to ensure the Department has the offensive and defensive capabilities and resources necessary to credibly deter adversaries from targeting the United States.

16. Do you believe that the Department possesses the necessary authorities to stand up an effective cyber deterrence posture? If not, what policies must be changed or added?

If confirmed, I look forward to reviewing the Department's relevant authorities. If, through that review, I see gaps in our ability to enable a more effective cyber deterrence posture, I would advocate for new or additional authorities with my leadership and this committee.

17. In your view, how do partners and allies contribute to developing and maintaining an effective cyber deterrence posture across the globe?

Secretary Hegseth has been clear that maintaining deterrence is not a mission the United States can achieve on its own. Cooperation in cyberspace with allies and partners underpins our ability to share sensitive information, facilitates cooperation on advanced capabilities, and allows us to secure the critical networks and infrastructure that facilitate our global posture. If confirmed, I would work to strengthen cyberspace cooperation with key partners around the world to ensure we collectively have the credible cyberspace capabilities required to deter and counter threats as they emerge.

18. What role do you see the relationship between space, cyber space, and nuclear escalation in the context of the U.S.'s strategic posture?

The relationship between space, cyber, and nuclear escalation is critical to our national security, and we must carefully manage the risks of escalation in each area. The Department cannot afford to view cyber in a silo; it must take an integrated and multi-domain approach to addressing the new and evolving challenges posed by our adversaries. Ensuring increased collaboration and integration of cyber with other non-kinetic capabilities will be particularly critical to securing the defense of our critical

systems and maintaining an offensive superiority over our adversaries.

If confirmed, I would collaborate with the ASD for Space Policy, the U.S. Space Force, and U.S. Strategic Command partners to enhance and solidify our nation's strategic posture in this complex environment. Specifically, I would focus on providing combatant commanders with integrated, multi-domain effects that reinforce deterrence and, if deterrence fails, maximize the lethality of the Joint Force.

19. 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?

Strong coordination between U.S. Northern Command and U.S. Cyber Command is essential for meeting the Department's missions and priorities to protect our nation. This partnership ensures U.S. Cyber Command contributes to the President's priority of defending the southern border from foreign threats to the homeland. The Commander of U.S. Northern Command is responsible for defense of the homeland and coordinates defense support to civil authorities. I understand that, where appropriate and consistent with the Secretary's direction, U.S. Cyber Command can provide limited cyber support domestically. At all times, U.S. Cyber Command's actions should be prioritized to the most significant threats facing the nation, including defending our southern border.

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.

20. What is your understanding of how DOD has been supporting, and being supported by, the National Cyber Director?

I understand that the Department of Defense works closely with the Office of the National Cyber Director (ONCD) to advance a whole-of-government approach to strengthening cybersecurity across the nation, involving efforts to develop and implement a comprehensive National Cyber Strategy. The Department is actively involved in disrupting and dismantling cyber threats by integrating cyber operations into broader campaigns designed to defend the nation in cyberspace.

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

If confirmed, I will work to further strengthen the partnership between the Department of Defense and the NCD to ensure alignment of the Department's strategic approach to cyberspace with national strategy. Department of Defense-NCD partnership should focus on achieving the President's and Secretary's vision of peace through strength. In my view, that means working together to craft and implement policies that strengthen critical infrastructure protection, strengthen the cyber workforce, and enhance engagement with

key partners in the private sector, academia, and the international community.

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

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

Transparent communication with Congress is critical to ensure Congress' ability to conduct oversight. I am aware that the Department of Defense updates Congress both through written notifications and regular briefings, through which we report on sensitive military cyber operations to the appropriate committees. If confirmed, I will work to ensure the Department consistently provides sufficient information for effective Congressional oversight.

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

If confirmed, one of my highest priorities will be to ensure the Department of Defense maintains regular engagements on cyber issues with Congress, to include supporting DoD's statutory responsibility for quarterly operations briefings to the defense committees. If confirmed, I commit to providing regular updates on military activities and operations in cyberspace.

2023 DOD Cyber Strategy

In 2023, DOD published its updated Cyber Strategy. It remains consistent with the belief that cyber is most effective when employed with other instruments of power as part of a larger campaign. It also uniquely highlighted the importance of global partners and allies as a force multiplier. Finally, it relays the continued threat to the defense industrial base, primarily from the People's Republic of China (PRC).

24. What elements of this strategy do you perceive as the most critical to meeting the demands of today's threat environment? Do you believe the Department is postured to fully execute this strategy? Please explain your answer.

I understand that the Department continues to take a strategic approach in the cyber domain that prioritizes defending forward against our adversaries in competition, in alignment with DoD capabilities and authorities, including engagement with allies and partners in cyberspace, improving force generation and intelligence support, and deepening integration of cyber into joint force lethality. If confirmed, I will review the Department's approach to cyber to ensure that it aligns to the President's objectives to defend the homeland, deter China, and increase burden-sharing with allies and partners. I

expect this review would likely uncover new opportunities to better integrate cyber operations with other kinetic and non-kinetic capabilities to reinforce the resilience and lethality of the Joint Force; enhance the adoption of cutting-edge private sector technologies that deliver military advantages; and accelerate actions to grow our cyber forces.

25. 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?

I understand that the Defense Industrial Base (DIB) faces a dynamic cyber threat landscape in which poor cybersecurity practices are rapidly exploited by capable and determined adversaries. As the Sector Risk Management Agency for the DIB, the Department has a responsibility to support efforts by DIB organizations to enhance their cybersecurity and resilience. If confirmed, I would look forward to engaging closely with partners at DoD, including the ASD for Homeland Defense and Hemispheric Affairs and the DoD CIO, as well as DIB companies to understand the current threats they face and opportunities for the Department to enhance the support it provides.

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

We must recognize the speed at which the AI landscape is evolving, and this rapid evolution requires that we keep pace. Artificial intelligence has the potential to improve vulnerability research and access development for cyber missions and accelerate the speed and scale of many aspects of conducting cyber operations.

If confirmed, I would focus on ensuring that AI is leveraged to ensure advantage for the Department. This means ensuring that our innovation and acquisition pathways are nimble and mission-focused, removing policy and institutional barriers that slow us down, and adapting our strategies and plans to nascent threats and opportunities. I also understand that seizing these opportunities will require workforce enhancements across the DoD enterprise. If confirmed, I will work with the DoD Chief Information Officer, as well as with operational components who use these capabilities on a daily basis, to ensure DoD leverages data and AI to gain full situational awareness in the cyber domain.

Deterrence of Cyber Attacks on US Critical Infrastructure

The 2023 Military Cyber Strategy and testimony from multiple administration witnesses affirm that the 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.

27. 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?

The President and the Secretary have made very clear that the Department must prioritize defending the homeland and deterring Chinese incursions into our infrastructure. Cyberattacks on U.S. critical infrastructure undermine each of these priorities. Cyberattacks that cause significant physical damage, disrupt critical national infrastructure, target civilians, or are clearly carried out with the intent to harm our economic or military capabilities could be viewed as an act of war, although this is a political calculation, as is the response to such actions. I believe any such hostile act should be met with a decisive and proportionate response, utilizing all instruments of national power at our disposal, in accordance with the law of armed conflict. If confirmed, I will ensure the United States is prepared to promptly leverage federal law enforcement agencies and generate response options as appropriate.

28. 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?

Under President Trump and Secretary Hegseth's leadership, I understand that DoD is laser-focused on restoring deterrence across all domains, including cyber, and will be assertive in addressing China's unacceptable intrusions on our civilian and government networks. China continues to invest in a broad arsenal of cyber capabilities, with the clear intention of challenging U.S. national interests at home and abroad. If confirmed, I would focus on engaging our operational commanders to present options for the Secretary and the President with a range of flexible yet decisive options that are directly tied to Joint Force objectives, while continuing to invest in efforts across the Department of Defense to fortify our cyber defenses. I would also focus the Department's actions on contributing to whole-of-government efforts to enhance deterrence as well as our domestic cybersecurity and resilience.

29. 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?

China's malicious cyber activities threaten American interests and undermine our ability to fight and win This behavior is unacceptable. If confirmed, I will seek to ensure that we are appropriately leveraging our world-class cyber capabilities to deter Chinese behavior and, as necessary, act effectively and resolutely in cyberspace.

30. 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?

Under President Trump and Secretary Hegseth's leadership, I understand that DoD is laser-focused on restoring deterrence across all domains, including cyber, and will be assertive in addressing China's unacceptable intrusions on civilian and government networks. While increasing our offensive cyber capabilities is critical, DoD must also remain vigilant in defending its own networks and critical infrastructure, in partnership with other U.S. Government departments and agencies. If confirmed, I would continue to ensure the Department has the robust, effective, and second-to-none offensive and defensive cyber forces and capabilities necessary counter these activities.

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

As the Sector Risk Management Agency (SRMA) for the Defense Industrial Base (DIB), DoD contributes to a whole-of-government model for national critical infrastructure protection and resilience. If confirmed, I would make it a priority to support requests for assistance from federal civilian agencies or the private sector through appropriate channels.

32. What is your understanding of how the process for Defense Support to Civil Authorities (DSCA) works when other agencies request cyber support from DOD? Do you believe any authority or policy processes need to be updated to make that process more agile and responsive?

The Department of Defense plays a crucial role in supporting civil authorities during emergencies and crises by providing Defense Support of Civil Authorities (DSCA) assistance. This support is activated at the direction of the President or upon approval by the Secretary of Defense, typically in response to requests from lead federal agencies overwhelmed by crises, natural disasters, or special events requiring unique military capabilities. As a key priority, if confirmed, I will work closely with the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs to ensure prompt and thorough reviews of all DSCA requests.

33. Section 1511 of the FY23 NDAA clarified the authority of the President to authorize USCYBERCOM to conduct activities to safeguard or defend critical infrastructure. What is your understanding of the Department's efforts to develop or issue any guidance related to that authority in the event it should ever be used?

I agree that safeguarding and defending critical infrastructure is important for U.S. national security. I have not had the opportunity to review DoD's activities to support Section 1511 of the NDAA for FY 2023. If confirmed, I would carefully review DoD's activities to safeguard or defend critical infrastructure and make recommendations to ensure it is able to conduct its role effectively.

34. Section 1517 of the FY24 NDAA established a pilot program for DOD to better understand the operational challenges to protecting and managing defense critical infrastructure necessary to support military operational plans under cyber attack situations. What is your understanding of the status of this pilot program?

I agree that protecting and managing defense critical infrastructure is necessary for supporting military operational plans and protecting them from cyber attack. I have not had the opportunity to review DoD's activities to support Section 1517 of the NDAA for FY 2024. If confirmed, I would carefully review DoD's activities to launch this pilot program and make recommendations to ensure it is able to conduct its role effectively.

35. 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 DHS or other Federal agencies may seek cyber support from DoD components through a formal Defense Support to Civil Authorities request. This mechanism is designed to support crisis response when other Federal, State, or local capabilities are exceeded or when required capabilities do not exist outside DoD. I further understand that DoD participates in a whole-of-government model for responding to significant cyber incidents. If confirmed, I would look forward to engaging with my interagency counterparts to better understand how DoD's unique capabilities and authorities can support national preparedness and resilience efforts.

36. In your view, how does cybersecurity of operational technology (OT) contribute to defense of critical infrastructure? What are the requirements you believe the Department needs to satisfy to ensure they are postured to secure OT?

The cybersecurity of operational technology is essential to ensure that DoD can project power and accomplish its missions during a time of crisis or conflict. If confirmed, I would focus on engaging Component heads across DoD to understand their requirements in this area and ensure they have everything they need to secure defense of critical infrastructure.

Dual Hatting of Commander, CYBERCOM

37. 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 understand that the dual-hat relationship places the same individual in charge of the National Security Agency (NSA) and U.S. Cyber Command. NSA and U.S. Cyber Command have distinct but complementary missions in the cyber domain. These are

incredibly important responsibilities for intelligence and defense, and must be coordinated. As U.S. Cyber Command continues to mature, its relationship with NSA should be continuously evaluated to ensure that each organization's primary mission is executed with maximum efficiency and effectiveness. If confirmed, I will support continued consultations with the Secretary of Defense and Congress on this issue and work to ensure our institutions are optimized to defend the nation and advance American interests.

38. 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?

I understand that the National Security Agency and U.S. Cyber Command have distinct but complementary missions in the cyber domain to advance and defend U.S. national interests. The enhanced coordination between NSA and U.S. Cyber Command is underpinned by a series of support agreements, memoranda of understanding, and special partnership agreements. These agreements and processes ensure that the separate roles, resources, and responsibilities of these two organizations are clearly defined, optimized, and mutually reinforcing. If confirmed, I am committed to ensuring that USCYBERCOM and NSA fulfill their distinct, critical missions, and amplify one another's efforts in defense of the nation.

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 last year.

39. If confirmed, what role do you foresee playing in influencing policy and resource allocation to ensure appropriate funding for cyber operations and capabilities?

If confirmed, I view the EBC authority granted under Section 1507 as a pivotal opportunity to strengthen our nation's cyber posture. My primary role will be to ensure this authority is used to proactively shape a cyber force that is prepared to deter, defend, and, when directed, defeat adversaries in the digital domain.

Specifically, I will focus on three key areas: First, accelerating the development and deployment of advanced cyber capabilities, particularly in areas like access technologies, offensive cyber options, and resilient infrastructure. Second, investing in our people, attracting, retaining, and developing a highly skilled cyber workforce through robust training pipelines and competitive compensation. And third, enhancing our partnerships with interagency, industry, and international allies and partners to achieve a more unified and effective cyber defense.

Through USD(P), I intend to work closely with the DoD Comptroller, CAPE, CIO, the Military Departments and Services, and Congress to ensure transparency and accountability in our budget decisions. My commitment is to deliver maximum cyber effect for every dollar invested, and to ensure that our resource allocation directly supports national security priorities.

40. If confirmed, how do you intend to maintain 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?

If confirmed, I will prioritize strengthening reporting and oversight of all cyber-related funding – both within the Enterprise IT and Cyber Activities (IT/CA) budget and across the broader Department. Additionally, it is my understanding that the ASD(CP), as the Principal Cyber Advisor (PCA) to the Secretary of Defense, has a statutory responsibility, outlined in 10 U.S.C. § 392a, to review and certify the adequacy of the Department's cyber operations budget to the Secretary of Defense. I understand that the ASD(CP), in his or her capacity as the PCA, coordinates and works closely with the DoD Chief Information Officer, who has similar statutory authority with respect to the Department's cybersecurity budget.

If confirmed, I intend to build upon this foundation, through USD(P), by proactively collaborating with the DoD Comptroller and the Office of Cost Assessment and Program Evaluation to enhance the PCA's role throughout the Planning, Programming, Budgeting, and Execution (PPBE) process – particularly during the critical Program Objective Memorandum (POM) and Program Budget Review (PBR) phases. Crucially, this would require close coordination with the Commander of U.S. Cyber Command, the Military Department Secretaries, the Military Department Principal Cyber Advisors, and the heads of defense agencies.

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).

41. 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?

The Department of Defense relies heavily on Science and Technology (S&T) investments to maintain a competitive edge in cyberspace. Organizations like the Defense Advanced Research Projects Agency (DARPA), the Strategic Capabilities Office (SCO), and the service labs have a proven track record of developing cutting-edge technologies that directly translate into enhanced cyber capabilities. These organizations play a vital role in ensuring our warfighters have the tools they need to operate effectively in this dynamic domain.

If confirmed, I am committed to fostering strong partnerships with key stakeholders to further leverage S&T for cyber advantage. I will work closely with the Military Department Principal Cyber Advisors and other senior leaders to identify and prioritize service-sponsored S&T initiatives that offer the greatest potential to strengthen our cyber posture. Furthermore, recognizing the criticality of rapid transition from research to operational capability, I will explore modifications to Enhanced Budget Control mechanisms to facilitate streamlined funding and acquisition processes for promising cyber S&T projects. This will ensure that breakthroughs in areas like artificial intelligence, quantum computing, and advanced persistent threat mitigation can be quickly deployed to enhance our cyber defenses.

Additionally, I will actively coordinate with the Under Secretary of Defense for Research and Engineering, DARPA, and SCO to advocate for appropriate S&T investments within the annual programming guidance and Future Years Defense Program (FYDP). This collaborative approach will ensure alignment between S&T efforts and the Department of Defense's overall cyber strategy, maximizing the return on investment and delivering the most effective capabilities to our cyber forces. This includes advocating for adjustments to future FYDPs to reflect the dynamic nature of the cyber domain and the need for agile resource allocation to address emerging threats and technologies. I believe the Department must ensure that its budget process, including Enhanced Budget Control considerations, remains flexible enough to adapt to the rapidly evolving cyber landscape.

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.

42. 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 the Department, in response to section 1533 of the National Defense Authorization Act for FY 2023, is developing a new cyber force generation model informed by relevant aspects of USSOCOM and JSOC's organizational structures. I believe that it will be critical for the Department to have a highly capable and consistently ready cyber force, focused on achieving excellence and mastery, to counter the growing threats posed by China and other malicious cyber actors. Any decision involving a separate cyber service must focus on developing the most capable cyber force for the Department, able to meet our pacing cyber threats.. I believe that a critical aspect of any potential future cyber force efforts is ensuring the Department fully evaluates the

resources and tradeoffs required to establish a separate service. If confirmed, I will work to ensure these efforts align with the Secretary's vision to restore the warrior ethos and rebuild our military. I look forward to working with Congress throughout these important policy decisions.

43. 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 understand the Department is evaluating options to improve Cyber Mission Force readiness, and that the Services have already made significant progress. The Military Services have the ability to track their personnel by USCYBERCOM personnel work roles in response to NDAA for FY 2024 House Report 118-125 on H.R. 2670. The Cyber Mission Force work role coding and tracking enables better ability to identify staffing gaps and optimize assignment management. I believe DoD can utilize section 1535 of the FY 2024 National Defense Authorization Act to address many of the readiness shortfalls identified across the Services. If confirmed, ensuring the Cyber Mission Force's sustained readiness will be a top priority. I will also work with the Services and other relevant organizations within the Department of Defense to address the multiple challenges impacting readiness.

44. As CYBERCOM 2.0 evaluates various force presentation models, should the Department and Congress provide CYBERCOM with additional personnel management authorities to solve these readiness problems?

I understand that Congress has granted the Department flexible personnel management tools to address cyber force readiness challenges. These tools include the Cyber Excepted Service, specialized cyber-peculiar awards, and USCYBERCOM's authority to recruit and hire experts in science, engineering, and other fields under Title 10 U.S. Code, Section 4092. If confirmed, I will assess the existing authorities and collaborate with Congress on any additional authorities needed to ensure the cyber force maintains a high state of readiness.

45. If confirmed, 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 thoroughly review the Department's current personnel management authorities to ensure they are being used to their fullest potential. I will collaborate with the DoD CIO and the Under Secretary of Defense for Personnel and Readiness to conduct this evaluation and work with USCYBERCOM and the Military Services to address any shortcomings in developing and sustaining a robust cyber workforce, encompassing both military and civilian personnel.

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."

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

During my time at USCYBERCOM and as a professional staff member in Congress, I observed many efforts that have yielded improvements in Service training, recruiting, and retention for the Cyber Mission Force (CMF). While the overall readiness trends are positive, the readiness initiatives have not been applied consistently across each Service. If confirmed, I will make high CMF personnel readiness a priority, and I will work with the Services, USCYBERCOM, and other Department stakeholders to leverage best practices to continue to drive sustained readiness.

47. 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 will prioritize implementing Section 1533 of the National Defense Authorization Act for FY 2023, including implementing a revised cyber force generation model to ensure the Services provide necessary personnel to the Cyber Mission Force (CMF). Recognizing the Services use varying readiness tracking databases, I will focus on leveraging existing tools to gain DoD-wide insights. If confirmed, I will work with USCYBERCOM and the Services to assess and, if necessary, update the Department's current readiness policies and processes to best enable our CMF readiness.

48. If confirmed, how will you work with the Services, their principal cyber advisors, and the cyber service components to not only meet the current readiness targets but also build the future force, as articulated within CYBERCOM 2.0?

If confirmed, I would work with key stakeholders within the Department to ensure we are developing a highly skilled cyber workforce. I will coordinate with the Services and USCYBERCOM to identify and implement effective strategies for recruiting and retaining the skilled cyber workforce necessary to achieve and maintain sustained readiness. While the Services have made significant progress in establishing foundational readiness across the cyber force, continued investment is essential to build on this momentum and reach enduring readiness goals for the future force. Additionally, I will collaborate with USCYBERCOM to ensure the Department establishes readiness targets that are aligned with and drive improved operational outcomes.

49. In your view, what are the most critical personnel issues that you think need to be addressed during this Administration to counter China?

Our people are critical to any potential conflict, especially with adversaries like China. While investing in technology is essential, building a highly skilled cyber force is equally important. This requires prioritizing recruitment, advanced training, and retention of specialized cyber personnel. The rapidly evolving cyber domain demands an agile and adaptable workforce. Therefore, the Department must develop and implement specialized, mission-focused training to counter emerging threats and maintain superiority. The Department must also evaluate different workforce models to ensure we effectively leverage all resources—military, civilian, contractors, National Guard, and Reserve. If confirmed, I will work with the Services and USCYBERCOM to enhance our cyber workforce and effectively counter China.

Development of Cyber Capabilities

While efforts continue to grow in building organic capabilities, trade craft, technology, training, and equipment, CYBERCOM has depended on NSA to build a strong foundation from which they are able to conduct cyber operations.

50. 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.

The Department has made strides in cyber innovation, but improvement is needed. We must streamline processes, particularly between the JCWA PEO and initiatives like the Constellation program conducted in partnership between US Cyber Command and DARPA to foster broader collaboration. If confirmed, I will prioritize agile resourcing, alternative funding models, and the seamless integration of programs like Constellation into the DoD's overall cyber strategy.

However, simply having these tools is not enough. A key challenge remains in ensuring seamless integration and rapid translation of S&T breakthroughs into operational capabilities. Silos still exist, and the pace of innovation often outstrips our ability to field new solutions quickly.

If confirmed, I will prioritize identifying and addressing any potential friction points. This would include working closely with the Commander of U.S. Cyber Command and the Joint Staff to proactively assess capability gaps, streamline acquisition pathways, and advocate for sustained investment in both foundational research and rapid prototyping. I will also prioritize ensuring that operational feedback is included early in capability development efforts. My focus would be on fostering a more agile and responsive ecosystem that can consistently deliver cutting-edge cyber capabilities to our warfighters.

51. 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?

I understand that the establishment of the Program Executive Office for the Joint Cyber Warfighting Architecture (per Section 1509, of National Defense Authorization Act for FY 2023) and the granting of Systems Engineering and Integration authority to U.S. Cyber Command by the Office of the Under Secretary of Defense for Acquisition and Sustainment in July 2023 are critical steps. While U.S. Cyber Command controls cyber capability requirements and possesses enhanced budget authority, the process for granting Milestone Decision Authority is progressing as planned. JCWA is crucial for rapidly adopting, maturing, and transitioning innovative cyber technologies into operational capabilities. The CYBERCOM Revised Cyber Force Generation Model's organizational, technical, and programmatic functions will align with and optimize resource delivery for the Joint Cyber Warfighting Architecture. If confirmed, I will prioritize working with the Office of the Under Secretary of Defense for Acquisition and Sustainment and U.S. Cyber Command to expedite the Program Executive Office's establishment and advance the Joint Cyber Warfighting Architecture's development, essential for ensuring our nation's cyber superiority.

52. 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?

Advocating for robust service-level S&T funding for cyber research will be a top priority for me, if confirmed. I will review, in partnership with the Under Secretary of Defense for Research & Engineering (R&E) and the Chief Information Officer (CIO), the current department-wide investments to determine the right governance structure to prioritize cyber S&T investments across the Department. This review will include examining whether it would be more effective to include S&T in Enhanced Budget Control (EBC) and aligning those efforts more closely with the Defense Innovation Unit (DIU) to accelerate transition from research to operational capability.

My approach would be two-fold. First, I would work directly with the Military Department Principal Cyber Advisors to rigorously assess service-sponsored S&T proposals, ensuring they align with the Department's overarching cyber strategy and address identified capability gaps. I would then champion these high-priority initiatives during the PPBE process, making a clear case for their value to senior DoD leadership.

Second, I would actively partner with the Under Secretary of Defense for Research and Engineering to shape Department-wide S&T guidance, ensuring cyber research receives appropriate prioritization and resources. This collaboration would be crucial in fostering a cohesive, Department-level approach to cyber innovation, maximizing our collective impact and accelerating the development of the capabilities our forces need to maintain a decisive edge.

53. Where do you think you can rely on the S&T activities of the other elements of DOD to support CYBERCOM and DOD-wide and military service cyber capabilities?

DOD S&T offers crucial support to USCYBERCOM and military cyber capabilities across the other four warfighting domains including air, land, maritime, and space. We can leverage research from organizations like DARPA and OUSD(R&E) to explore cutting-edge technologies like quantum computing and advanced algorithms. The services and other agencies can then transition this research into practical offensive and defensive tools. Rigorous testing and evaluation within existing DOD infrastructure ensures these tools are effective and resilient. If confirmed, I will ensure close collaboration and information sharing across the department to prevent redundancy and maximize the impact of our S&T investments. Furthermore, recognizing the criticality of rapid transition from research to operational capability, I will explore modifications to Enhanced Budget Control mechanisms to facilitate streamlined funding and acquisition processes for promising cyber S&T projects.

54. What role do you believe private industry plays in developing technical capabilities and advanced technology to support cyber operations? In your view, is the Department postured to take advantage of industry at the speed required?

I understand the Department has a critical shortage of skilled acquisition professionals to manage the development of complex cyber capabilities, despite ongoing Department-wide efforts to recruit and retain such talent. If confirmed, I will address this challenge by working through USD(P) with USD(P&R), USD(A&S), the Defense Acquisition University, and the DoD CIO to strengthen the cyber acquisition workforce. This will include leveraging talent exchanges and career broadening opportunities, cultivating talent pipelines within both the acquisition workforce and the Cyber Excepted Service, and enhancing training and information sharing, as directed by initiatives like Section 835 of the NDAA for FY 2023 and the DoD Cyber Workforce Strategy. My focus will be on developing a robust and skilled cyber acquisition workforce to support Cyber Command's mission.

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. Successful management of the development of highly integrated and agile cyber capabilities will require personnel who have expertise not only in systems acquisition but also in advanced technology. Congress has thus stressed the need for the leadership in the Department to assist CYBERCOM in acquiring this expertise.

55. 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?

I understand the Department has a critical shortage of skilled acquisition professionals to manage the development of complex cyber capabilities, despite ongoing Department-wide efforts to recruit and retain such talent. If confirmed, I will address this challenge by working with USD(P&R), USD(A&S), the Defense Acquisition University, and the DoD CIO to strengthen the cyber acquisition workforce. This will include leveraging talent exchanges and career broadening opportunities, cultivating talent pipelines within both the acquisition workforce and the Cyber Excepted Service, in alignment with the DoD Cyber Workforce Strategy.

Artificial Intelligence for the Cyber Mission Force

Section 1554 of the National Defense Authorization Act for Fiscal Year 2023 tasked United States Cyber Command to develop a five-year roadmap and implementation plan for rapidly adopting and acquiring artificial intelligence systems, applications, and supporting data for cyberspace operations forces. In early 2024, the Command delivered this roadmap and implementation plan to Congressional committees. While there has been progress against this plan, the rapidly evolving threat environment, particularly with the release of DeepSeek R1, demands a more rapid adoption and fielding of this technology.

56. What role do you foresee playing in advocating for funding and developing policy for the use of artificial intelligence capabilities in the cyber domain?

I believe that AI technologies have the potential to augment the capabilities of our cyber forces and contribute to decisive warfighting advantages. Given the rapid evolution of the AI ecosystem, DoD will only realize this potential if it can move with speed and agility to identify, test, and field these capabilities. I further believe that this is an area in which the Department must continue to work closely with private sector partners in industry and academia. If confirmed as ASD(CP), I would collaborate closely with U.S. Cyber Command, the Chief Digital and Artificial Intelligence Office (CDAO), DARPA, and Defense Innovation Unit, to look for ways we can accelerate the adoption of AI to support cyberspace operations forces.

57. If confirmed, how will you work to decrease the time from identification of a requirement or tool for evaluation, to acquisition of that specific capability and fielding of these critical technologies for cyberspace operations?

The Secretary has made clear that rapidly identifying, acquiring, and fielding cutting-edge technologies is critical to restoring our warfighting advantages. This is true in cyberspace as well as in other domains. We must also ensure that our acquisitions processes operate with efficiency, prioritizing lethal and cost-effective capabilities that

directly support our core strategic objectives. If confirmed as ASD(CP), I would work closely with partners across the Department, as well as in industry and in academia, to assess how best to use rapid acquisition pathways to support cyberspace operations forces.

58. How do you intend to work with industry, as well as partners like CDAO, the services and DARPA, to bring the most current artificial intelligence technologies to cyber operators across all mission types?

I believe that close collaboration with partners across the innovation ecosystem, both within and external to government, is critical to the Department's ability to field cutting-edge technologies that enable warfighting advantages. If confirmed as ASD(CP), I would work closely with U.S. Cyber Command, CDAO, DARPA, and Defense Innovation Unit, and other Department stakeholders to seek opportunities accelerate the adoption of AI and other critical technologies to support cyberspace operations forces.

Intelligence Support for Challenging Cyber Targeting Requirements

The Fiscal Year 2025 National Defense Authorization Act directed the Department to establish a dedicated cyber intelligence capability no later than October 2026. Foundational intelligence support is critical for the success of cyber operations conducted in support of Combatant Command Operational Plans in competition, conflict, or crisis. 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).

59. What is your understanding of the importance of foundational intelligence to cyber operations, and the current challenges in adequate support for such requirement?

I believe intelligence support is the cornerstone of effective cyber operations. I understand that U.S. Cyber Command and the Defense Intelligence Agency have been working together on this problem, and if confirmed I look forward to better understanding the key findings provided to Congress. I also consider the NDAA for FY 2025 requirement to stand up a dedicated cyber intelligence capability an important step toward ensuring the broad resources of the Defense Intelligence Enterprise are available to support the cyber warfighter. There is more work to be done to ensure intelligence supports the cyber warfighter, and I look forward to taking on this challenge.

60. If confirmed, how will you work 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 on this requirement?

I believe the ASD for Cyber Policy has a key role to advise the Secretary on any challenges impeding our ability to present the Secretary and President with credible and effective cyber options across the continuum of conflict. If confirmed, I will review the work that has already been done by the Department and Intelligence Community to address this problem. From there, I would look to evaluate how the lack of foundational intelligence has impacted the joint force in executing both offensive and defensive cyber operations. I would also examine what steps are available under present authorities to improve the provision of this intelligence support, such as enhanced information sharing and human capital development. If confirmed, I will work with the Commander of U.S. Cyber Command, the Under Secretary of Defense for Intelligence and Security, and other key stakeholders to identify a way forward that will enable us to develop and maintain a robust set of capabilities for both deterrence and in wartime.

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.

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

The Department of Defense can play an important role in whole-of-government efforts to deter hostile information operations directed against the United States, its allies, and interests. If confirmed, I look forward to reviewing the Department's role in this area and will seek to ensure our efforts support the President's priorities, and protect the United States, the American people, and our national interests against hostile information operations while upholding the highest standards of respect for our Constitution.

62. If confirmed, how would you engage across interagency partners to develop needed policy to defend against such operations?

I agree that effective policy is needed to enable the Department to combat hostile information operations and malign influence. If confirmed, I look forward to better understanding the role of cyber in defending against such operations in an effort to ensure our efforts support the President's priorities.

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.

63. 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?

The President has been clear that we must restore peace through strength. I believe cyber presents an opportunity to achieve the President's objectives. If confirmed, I will work to ensure DoD is appropriately investing in cyber information operations and capabilities, incorporating lessons learned, and enhancing our cyber warfighters' ability to operate with maximum lethality, agility, and efficacy.

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

I believe that the Principal Information Operations Advisor (PIOA), the senior advisor to the Secretary of Defense on all information operations (IO) matters, has the lead responsbility for aligning DoD policy and oversight of cyber and information operations. The PIOA focuses on integrating IO expertise, overseeing related policies and strategies, and ensuring coordination across the DoD. If confirmed, I will thoroughly examine the distinct responsibilities of each role and review examples of their joint efforts to both sustain current cooperative practices and identify opportunities for improvement.

65. What is your understanding of the term narrative intelligence and what role do you believe it would play in successful information operations?

I understand narrative intelligence to refer to insights gleaned from the narratives that adversaries use to drive information operations. If confirmed, I look forward to better understanding how this type of analysis could enhance information operations.

66. 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 believe strongly in the need to ensure the Department's cyber operations are integrated and layered with other non-kinetic and kinetic capabilities to maximize their strategic impact. If confirmed, I look forward to better understanding the Department's concepts for integrating cyber with other tools of national power and ensuring our warfighters can operate with the greatest possible lethality, agility, and efficacy.

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

If confirmed, I look forward to working with the PIOA to learn more about how the Department measures effectiveness of DoD information operations and understanding the role that cyber plays.

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

If confirmed, I will work with the PIOA to determine whether additional authorities or resources are necessary to effectively execute the Department of Defense's missions, and I will communicate any findings I might have to the Secretary and to Congress.

69. 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?

Close collaboration between the Principal Cyber Advisor (PCA) and the Principal Information Operations Advisor (PIOA), the senior advisor to the Secretary of Defense on all information operations (IO) matters, is crucial for aligning DoD policy and oversight of cyber and information operations. The PIOA focuses on integrating IO expertise, overseeing related policies and strategies, and ensuring coordination across the DoD. If confirmed, I will thoroughly examine the distinct responsibilities of each role and review examples of their joint efforts to both sustain current cooperative practices and identify opportunities for enhancement.

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.

70. 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?

Cyber and information operations are often complementary, and most impactful when layered to deliver maximum effects. If confirmed, I would review the current assigned responsibilities and how they align with the priorities of President Trump and Secretary Hegseth. I will prioritize ensuring that the Department of Defense is fully leveraging non-kinetic effects to advance and defend our national interest. If, after review, I believe changes to responsibilities would materially improve mission outcomes, I will communicate those to the Secretary and to Congress.

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.

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

I understand that Section 1510 of the NDAA for FY 2023 mandates that USD(R&E) develop a force planning activity for non-kinetic effects, including the necessary command and control processes. Cyber forces will be crucial to this effort. If confirmed as ASD(CP), I will actively support this analysis and its implementation, ensuring effective integration of cyber capabilities into the Department's non-kinetic strategy.

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

If confirmed as ASD(CP), I will work to ensure the non-kinetic force planning activity fully integrates cyber capabilities, addressing cyber-specific requirements (including command and control, intelligence, and resourcing), and synchronizes cyber planning efforts across DoD. This includes aligning the plan with the interim National Defense Strategic Guidance and incorporating innovative concepts and emerging technologies. I will also address potential integration challenges, such as legal authorities and interagency coordination, and advocate for metrics to assess effectiveness. Finally, I will emphasize workforce development needs and explore opportunities to leverage international partnerships.

Red Team Modernization

Despite Cyber Red Teams playing a critical role in DOD's cybersecurity mission, governance of their activities remained unclear. Following issuance of two Congressionally mandated studies, the DOD CIO released an instruction on Cyber Red Teams in early 2024 outlining responsibilities for development, resourcing, and guidance. While principal cyber advisors were identified in the instruction, the yet-to-be established Assistant Secretary of Defense for Cyber Policy was absent.

73. What role do you believe the Assistant Secretary of Defense for Cyber Policy should have in the governance of cyber red teams?

I understand that DoD Cyber Red Teams provide valuable, independent insights into the Department's vulnerabilities and help to increase our overall cyber posture. If confirmed as ASD(CP), I would work closely with the DoD CIO, as well as U.S. Cyber Command, the Military Department's Principal Cyber Advisors, and the DoD Cyber Red Team community to ensure we continue to work together to strengthen its governance.

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

The DoD Cyber Red Teams are a crucial part of a robust cyberspace defense strategy, providing valuable, independent insights into the Department's vulnerabilities and helping increase our overall cyber posture. If confirmed, I look forward to working with the DoD CIO, U.S. Cyber Command, and the DoD Cyber Red Team community to ensure that the Department is aligning its efforts to the Secretary's top priorities.

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

If confirmed, I will work to incorporate skill development of these teams into my training oversight responsibilities in coordination with DoD CIO and U.S. Cyber Command, to build and maintain a strong, capable, and healthy Red Team workforce that effectively identifies vulnerabilities and enhances the overall cybersecurity posture of the DoD. I will also ensure that the resourcing of these teams is aligned to the Secretary's top priorities, through my budget certification responsibilities.

<u>Cybersecurity of the Nuclear Command, Control, and Communications Network</u>

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.

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

The security and resilience of the nation's NC3 systems is a no-fail mission for the Department of Defense. If confirmed, I would make it a top priority to prioritize the cybersecurity of the NC3 enterprise. Doing so would likely involve convening all Department stakeholders to assess risks to NC3 systems and ensure that appropriate mitigations are in place. I would further look forward to working with Congress to provide regular updates and align resources and authorities.

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

I understand the Secretary has established a cross-functional team to assess cyber risks to NC3 systems and implement mitigations, as appropriate. If confirmed, I would prioritize support for this effort in an effort to ensure that I and my team are closely aligned with key stakeholders from across the Department.

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.

78. 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?

While the DoD CIO is the principal advisor to the Secretary and Deputy Secretary of Defense for information enterprise matters, including cybersecurity, I believe that decisions about adopting requirements like SBOMs should not be made in isolation. If confirmed as ASD(CP), I would actively engage in such decisions, given their potential impact on the Department's cybersecurity posture, and ensure that the Military Department PCAs and their respective Military Department CIOs are included in a collaborative approach to this topic.

79. What are your views about adoption of a policy of requiring SBOMs and how it might support the cybersecurity missions of the Department?

I believe SBOMs offer valuable information into software supply chains, providing program managers and cybersecurity personnel with critical information to manage risk, particularly given the modular nature of modern software and its potential vulnerabilities. If confirmed, I will work with the DoD CIO, the Military Department PCAs, and their respective Military Department CIOs on adoption of the 2023 DoD Software Modernization Implementation Plan across the Department.

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.

80. 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.

81. 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.

82. 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.

83. 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.

84. 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.

85. 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.

86. 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.