Advance Policy Questions for Lieutenant General Joshua M. Rudd, USA
Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service

Duties and Qualifications

1. **What is your understanding of the duties and functions of the Commander, U.S. Cyber Command?**

The Commander of U.S. Cyber Command (USCYBERCOM) is charged with leading the Department's unified effort in the cyberspace domain. This involves directing, synchronizing, and coordinating military cyberspace operations to defend and advance our national interests. Key responsibilities, as outlined in Title 10 U.S.C. §167b and the Unified Command Plan, call for USCYBERCOM to serve as the Joint Force Provider, Joint Force Trainer, and execute Enhanced Budgetary Control in order to secure and defend the Department of Defense Information Network (DoDIN), provide combat-ready cyber forces to the other Combatant Commands, and execute the full spectrum of cyberspace operations to deter adversaries and support Joint Force objectives.

2. **What is your understanding of the duties and functions of the Director of the National Security Agency/Chief of the Central Security Service?**

The Director of the National Security Agency (NSA) and Chief of the Central Security Service (CSS) leads the nation's premier cryptologic organization and is responsible for two core missions of vital importance to our national security: Signals Intelligence (SIGINT) and Cybersecurity. Under the authority of the Director of National Intelligence and the Under Secretary for Intelligence & Security, the Director oversees the SIGINT mission to produce critical foreign intelligence that provides decision advantage to our nation's leaders and warfighters. Concurrently, the Director leads the cybersecurity to prevent and minimize risks to our National Security Systems and the Defense Industrial Base. The Director also drives innovation in cryptography and advanced technologies to maintain the United States advantage over adversaries.

The Director concurrently serves as the Commander, USCYBERCOM and executes its combatant commander duties as defined by law and policy.

3. **What background and experience do you possess that qualify you to perform these duties?**

I have been privileged to serve for over three decades in leadership roles spanning the Joint Force, with extensive experience in the Indo-Pacific theater. My career has provided me with a deep, mission-driven understanding of the operational and strategic challenges we face, particularly concerning the pacing challenge of China.

As the current Deputy Commander of U.S. Indo-Pacific Command (USINDOPACOM), I have been responsible for integrating operations across all domains—including cyberspace—to reinforce deterrence and prepare to fight and win if deterrence fails. This role has given me firsthand insight into the operational needs of the warfighter and the critical importance of synchronizing cyber effects with kinetic and non-kinetic capabilities. My prior leadership positions in special operations and joint task forces have honed my ability to lead multidisciplinary teams, manage complex operations, assess risk, and build the strong relationships with allies and partners that are essential to prevailing in strategic competition. These experiences have prepared me to lead the men and women of USCYBERCOM and NSA and ensure their world-class capabilities and talent are fully leveraged and integrated to support our national security objectives.

4. **What qualifications do you have to command military forces and military operations?**

Throughout my 32-year career, I have had the honor of leading warriors in command at multiple echelons, from company through theater-level joint commands, in both peacetime and in combat. My experience as Deputy Commander of USINDOPACOM, the largest geographic combatant command, has given me extensive experience in the operational art of integrating joint and combined forces across a vast and dynamic theater.

I have led joint and special operations task forces, and my qualifications to command in this modern environment are rooted in a leadership philosophy centered on speed, creativity, innovation, and scale. These assignments have provided me with a deep appreciation for the responsibilities of command, including the critical need to man, train, and equip our forces while ensuring their readiness and well-being. My professional military education, combined with these operational leadership experiences, has prepared me to command the joint forces of USCYBERCOM and lead its vital military operations.

5. **Do you believe that there are any steps that you need to take to enhance your expertise to perform the duties of the Commander, U.S. Cyber Command or the Director of the National Security Agency/Chief of the Central Security Service?**

Absolutely. While my career has focused on leading joint warfighting forces, my most immediate priority, if confirmed, would be to immerse myself in the deep technical expertise resident at both USCYBERCOM and NSA/CSS. This means my first action would be to listen and learn from the world-class military and civilian personnel who execute this mission every day.

Second, I would build on my existing relationships and forge new ones across the interagency, with our industry partners, and with Congress to ensure our efforts are fully aligned.

To outpace our adversaries, we must leverage the innovation and expertise resident across the entire national security enterprise and in the private sector. As part of enhancing my expertise, I intend to prioritize continuously engage with key allies and partners, whose collaboration is essential for collective defense and effective deterrence in the cyberspace domain.

Relationships

6. **Section 162(b) of title 10, United States Code, provides that the chain of command runs from the President to the Secretary of Defense and from the Secretary of Defense to the commanders of the combatant commands. Other**

sections of law and traditional practice, however, establish important relationships outside the chain of command. Please describe your understanding of the relationship of the Commander, U.S. Cyber Command, to the following officials:

The Secretary of Defense

The Commander, USCYBERCOM performs duties under the authority, direction, and control of the Secretary and is directly responsible to the Secretary for the preparedness of the command to carry out its assigned missions. If confirmed, I will work closely with the Secretary in coordination with the Chairman of the Joint Chiefs of Staff.

The Deputy Secretary of Defense

The Deputy Secretary performs such duties and exercises such powers prescribed by the Secretary. The Deputy Secretary will act for and exercise the powers of the Secretary on behalf of the Secretary as warranted. If confirmed, I will work closely with the Deputy Secretary, as appropriate, and keep the Deputy Secretary informed of USCYBERCOM missions and activities.

The Director of National Intelligence

As the head of the Intelligence Community, the Director of National Intelligence (DNI) acts as the principal advisor to the President and the National Security Advisor on intelligence matters pertaining to national security; and oversees and directs the implementation of the National Intelligence Program. The DNI coordinates national intelligence priorities, deconflicts and facilitates information sharing and coordination across the Intelligence Community. If confirmed, I will work closely with the DNI to ensure the intelligence community is responsive and timely with respect to the operational needs of USCYBERCOM.

The National Cyber Director

The National Cyber Director is the principal advisor to the President on cybersecurity policy and strategy, and leads whole-of-government coordination of policies to improve the cybersecurity posture of the United States, increase information and communications technology security, understand and deter malicious cyber activity, and advance diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace, among other matters. If confirmed, I look forward to working with the Office of the National Cyber Director in coordination with Department officials to integrate USCYBERCOM efforts with the rest of government to deter and disrupt cyber threat actors and build enduring advantage for the United States in cyberspace.

The Assistant Secretary of Defense for Cyber Policy and Principal Cyber Advisor to the Secretary of Defense

The principal duty of the Assistant Secretary for Cyber Policy is to develop and coordinate the Department's cyber strategy and policies. This position is responsible for ensuring alignment of the Department's cyber policy with national cyber policy and developing, implementing, and integrating cyber policy across the Department in support of the Under Secretary for Policy and the Deputy and Secretary. USCYBERCOM operates under the authority, direction, and control of the ASD for Cyber Policy, as assigned by law in Title 10 U.S.C. §167b. If confirmed, I look forward to working collaboratively with the Assistant Secretary for Cyber Policy and Principal Cyber Advisor (PCA) to the Secretary to defend the homeland, deter our adversaries, and ensure our nation's decisive advantage by providing policymakers with legally-sound options to deliver integrated effects.

The Department of Defense Chief Information Officer

The Department's Chief Information Officer (CIO) is the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary on policy, oversight, guidance, and coordination for all Department matters related to architecture and programs related to the networking and cyber defense architecture of the Department; information assurance; information resource management; information technology; electromagnetic spectrum, including coordination with other federal agencies and industry; coordination for classified programs; and in coordination with the Under Secretary for Personnel and Readiness and the PCA, policies related to the Cyber Operations Force (COF); for nuclear command and control systems; positioning, navigation and timing. Additionally, the CIO exercises authority, direction, and control over the Defense Information Systems Agency and the activities of the Cybersecurity Directorate of the NSA funded through the Information System Security Program. If confirmed, I look forward to working closely with the CIO on matters regarding USCYBERCOM's and NSA's responsibilities.

The Under Secretary of Defense for Policy

The Under Secretary for Policy (USD(P)) is the PSA and advisor to the Secretary and Deputy Secretary for matters regarding the formulation of national security and defense policy, and the integration of Department policy, strategy, plans, execution, and capabilities to achieve national security objectives. If confirmed, I look forward to working closely with the USD(P) on all policy issues affecting USCYBERCOM and NSA.

The Under Secretary of Defense for Intelligence and Security

The Under Secretary for Intelligence & Security (USD(I&S)) is the advisor and PSA to the Secretary and Deputy Secretary for all intelligence, counterintelligence, security, sensitive activities and other intelligence-related matters. Moreover, the USD(I&S) exercises authority, direction, and control on behalf of the Secretary over the NSA/CSS. The USD (I&S) also exercises authority, direction and control over the Defense Intelligence Enterprise, and serves as the Director of Defense Intelligence and principal advisor to the DNI on Defense Intelligence matters. If confirmed, I look forward to working closely with the USD(I&S) on matters relating to USCYBERCOM's and NSA's responsibilities.

The Chairman of the Joint Chiefs of Staff

The Chairman of the Joint Chiefs of Staff (CJCS) is the principal military advisor to the President, National Security Council, and Secretary. Communication between the President or the Secretary and the Combatant Commanders flows through the Chairman. By custom and tradition, and as instructed by the Unified Command Plan, if confirmed, I would routinely communicate with and through the Chairman regarding matters within USCYBERCOM's and NSA's responsibilities to ensure that he remains fully informed and able to provide sound and timely military advice to senior policymakers.

The Secretaries of the Military Departments

The USCYBERCOM Commander's authority over assigned Service components is clear in the Goldwater-Nichols Act but requires close coordination with the Secretaries of the Military Departments to ensure that USCYBERCOM does not intrude upon the responsibilities of the Secretaries of the Military Departments. Close coordination between the USCYBERCOM Commander, the Assistant Secretary for Cyber Policy and Principal Cyber Advisor, and each of the Secretaries of the Military Departments is also essential for gaining and maintaining the Services' support to cyber operations forces as an integral part of the Joint Force.

The Chiefs of Staff of the Services

The Service Chiefs are charged with providing organized, trained, and equipped forces to be employed by Combatant Commanders in accomplishing their assigned missions. Additionally, these officers serve as members of the Joint Chiefs of Staff and as such have a lawful obligation to provide military advice. Individually and collectively, the Service Chiefs are a tremendous source of experience and judgment. If confirmed, I look forward to working closely and conferring regularly with the Service Chiefs.

The Principal Cyber Advisors of the Military Departments

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. If confirmed, I will collaborate with the Assistant Secretary for Cyber Policy to work closely with the Military Department PCAs to develop and implement Department-wide cyber policy and strategies.

The Director of the Cybersecurity and Infrastructure Security Agency

The Cybersecurity and Infrastructure Security Agency (CISA) Director is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience, facilitating collaboration and partnership between all levels of government, industry, educational institutions, and the American public to reduce risk to the nation's cyber and physical infrastructure. The CISA Director reports to the Secretary of Homeland Security and is also responsible for fulfilling the Secretary's responsibilities for the security of Federal information and information systems, except for National Security Systems. If confirmed, I look forward to continuing the close partnership each of my predecessors enjoyed with the CISA Director to deter, prevent and disrupt threats to the nation's information systems and critical infrastructure.

The Under Secretary of Defense for Acquisition and Sustainment

The Under Secretary for Acquisition and Sustainment (USD(A&S)) is the PSA and advisor to the Secretary for all matters relating to acquisition and sustainment in the Department and serves as the senior procurement Defense Acquisition Executive for the Department, with the mission of delivering and sustaining timely, cost-effective capabilities for the Armed Forces. Acting through the Command Acquisition Executive (CAE), the Commander of USCYBERCOM is responsible for the development, acquisition and (as applicable) sustainment of cyber operations-peculiar equipment, capabilities and services. If confirmed, in coordination with the PCA, I look forward to working closely with the USD(A&S) to ensure that the USCYBERCOM CAE executes the command's acquisition authorities consistent with Department policies in support of national priorities.

The Under Secretary of Defense for Research and Engineering

The Under Secretary for Research and Engineering (USD(R&E)) is responsible for overseeing the research, engineering, and technology development activities across the Department's enterprise to ensure technological superiority for the Department. If confirmed, I look forward to working closely with the USD(R&E), in coordination with the PCA, to drive innovation and accelerate the advancement of cyber capabilities, thereby ensuring we maintain dominance in cyberspace.

The Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs

The Assistant Secretary for Homeland Defense and Hemispheric Affairs (ASD (HD&HA)), under the authority, direction, and control of the USD(P), executes responsibilities including overall supervision of the homeland defense and Defense Support of Civil Authorities (DSCA) activities of the Department as well as defense continuity and mission assurance, and U.S. defense and security policy for other nations in the Western Hemisphere. If confirmed, I look forward to working with the ASD(HD&HA) and the USD(P) on matters regarding USCYBERCOM's assigned responsibilities.

The Combatant Commanders, and, specifically, the Commanders of U.S. Strategic Command and U.S. Northern Command

The Commander, USCYBERCOM, has both supported and supporting relationships with other Combatant Commanders, largely identified within the Unified Command Plan, the Joint Strategic Capabilities Plan, execute orders, and operation orders. In general, the Commander, USCYBERCOM, is the supported commander for trans-regional and global cyberspace operations and is a supporting commander for cyberspace operations specific to a single Combatant Commander's area of responsibility. Specific relationships with the Commander, U.S. Northern Command, and Commander U.S. Strategic Command, will be delineated by the President or the Secretary in execute and/or operation orders. If confirmed, I look forward to working with the Combatant Commanders to deepen these relationships to support national and theater security objectives and to integrate effects.

The Director of the Defense Information Systems Agency/Commander of the Department of Defense Cyber Defense Command

The Director of the Defense Information Systems Agency/Commander of the Department of Defense Cyber Defense Command (DCDC) is a component, sub-unified command of USCYBERCOM that synchronizes and directs cyberspace operations and defense across the Department's Information Network. DISA is a combat support agency that operates and defends critical portions of the Department's Information Network while also providing critical enterprise services and capabilities. The two organizations are led by a dual-hatted Commander similar to the USCYBERCOM/NSA arrangement where each organization benefits from the capability and capacity of the other.

The Director of the Defense Intelligence Agency

The Director of the Defense Intelligence Agency (DIA) manages and executes specified Defense Intelligence and counterintelligence functions across the Defense Intelligence Enterprise and for select functions across the greater Intelligence Community. The DIA analyzes and disseminates military intelligence in support of combat and noncombat military missions and serves as the nation's primary manager and producer of foreign military intelligence. If confirmed, I look forward to working closely with the DIA Director on matters relating to USCYBERCOM's assigned responsibilities.

The Director of the National Reconnaissance Office

The Director of the National Reconnaissance Office (NRO) is the principal advisor on overhead reconnaissance to the Secretary, the Chairman of the Joint Chiefs of Staff, and the Combatant Commanders, responsible for developing, acquiring, launching, and operating space-based intelligence, surveillance and reconnaissance capabilities to secure and expand the U.S. intelligence advantage. If confirmed, I look forward to working closely with the NRO Director on matters relating to USCYBERCOM's assigned responsibilities.

The Chief Digital and Artificial Intelligence Officer

The Chief Digital and Artificial Intelligence Office (CDAO) is the Department's senior official responsible for the acceleration of adoption of data, analytics, and artificial intelligence (AI) to generate decision advantage. To this end, the CDAO leads strategy and policy on data, analytics, and AI adoption; provides oversight for efforts throughout the Department; develops digital and AI-enabled solutions at scale; and provides expertise to address urgent requirements and emergent challenges. If confirmed, I look forward to working closely with the CDAO, in coordination with other component heads in the Department and the Secretary's office, to integrate efforts to build enduring advantage for the Department and the nation.

Major Challenges and Priorities

7. **In your view, what are the major challenges that will confront the next Commander of U.S. Cyber Command?**

In my view, the major challenge facing USCYBERCOM is being postured to deter and, if necessary, defeat aggression from our strategic competitors in the cyberspace domain both in support of the Joint Force and in defense of the U.S. homeland. This requires meeting the multitude of cyber threats posed by China and Russia and other major adversaries; deepening the integration of cyber operations with the Joint Force; and ensuring the defense of our nation's critical infrastructure. A key challenge will be accelerating the development and fielding of advanced capabilities, ensuring that the command has the authorities necessary to counter our key adversaries, and building and retaining the elite and specialized talent required to prevail in this dynamic warfighting domain.

8. **In your view, what are the major challenges that will confront the next Director of the National Security Agency/Chief of the Central Security Service?**

From my perspective, the major challenges confronting the next Director of the NSA/CSS include the full spectrum of threats from China; the increasing volatility and the risk of crisis and conflict in multiple theatres; the accelerating technological change which can quickly alter the landscape on national security matters—especially in both Signals Intelligence (SIGINT) and cybersecurity; and the targeting of U.S. critical infrastructure and U.S. political and economic targets. The Director must ensure NSA/CSS remains the world's best SIGINT and cybersecurity agency providing exquisite intelligence and expertise for our nation. Balancing civil liberties and privacy concerns with effective intelligence gathering and maintaining strong partnerships with both domestic and international allies will also be critical. Additionally, attracting and retaining top talent to stay ahead of emerging threats in an increasingly competitive landscape poses a significant challenge.

9. **If confirmed, what plans do you have for addressing these challenges?**

If confirmed, I intend to focus on three mutually reinforcing lines of effort that apply across both USCYBERCOM and the National Security Agency.

- First, I will **sharpen our mission focus at scale** by aligning our resources, operations, and intelligence collection against the pacing challenge of China, the threat from Russia, threats to the U.S. homeland from both nation-state and non-state actors.
- Second, I will **accelerate innovation and integration**. This means driving the operational adoption of capabilities like AI and machine learning, deepening our partnerships with the private sector and thought leaders to stay ahead of the technology curve, and ensuring cyber is fully integrated with all other aspects of Joint Force operations.
- Third, I will **invest in people**. At both NSA and USCYBERCOM, the enduring advantage is the military, civilian, and contractor workforce. I will champion efforts to modernize training, develop more flexible career paths, and foster a culture of continuous learning to ensure we recruit and retain the elite talent our nation needs to secure its interests in cyberspace.

10. If confirmed, what will be your priorities for U.S. Cyber Command?

If confirmed, I will ensure USCYBERCOM is postured to fight and win our nation's wars and to effectively execute its mission in strategic competition. Pending the outcome of my 90-day review, I plan to:

1. **Sharpen Focus on the Pacing Challenge:** I will orient our operations, planning, and capability development to be postured for enduring homeland defense and to address the threat posed by China, ensuring the command is prepared to support the Joint Force in a potential conflict.
2. **Enhance Joint Force Lethality:** I will deepen the integration of cyber effects with combatant commands plans. Our ability to synchronize cyber operations with kinetic and non-kinetic effects across all domains is critical to ensuring the Joint Force can maintain freedom of action and achieve its objectives.
3. **Accelerate Modernization and Readiness:** I will prioritize the readiness of the Cyber Mission Force (CMF) and accelerate the acquisition and deployment of next-generation tools. To maintain our competitive edge, we must equip our elite warfighters with the advanced capabilities they need and ensure they are trained and ready to employ them.

11. If confirmed, what will be your priorities as the Director of the National Security Agency/Chief of the Central Security Service?

If confirmed, my priority as the Director of the NSA/CSS will be to ensure that both the SIGINT and cybersecurity missions of the Agency are fully aligned to support the priorities of the Secretary and the Director of National Intelligence. I will build upon the Agency’s extraordinarily talented workforce, ensure technological advantage in SIGINT and cybersecurity for the nation by deepening industry partnerships, and strengthen NSA’s extensive relationships across the U.S. Government, with a range of private organizations, and with key allies. Foundational to all of this, I will be committed to upholding the Constitutional rights and civil liberties of the American people in all Agency activities.

Relations with Congress

12. What are your views on the state of U.S. Cyber Command’s relationship with the Senate Armed Services Committee in particular, and with Congress in general?

Congress exercises its constitutional authority to oversee U.S. cyberspace missions through mechanisms of accountability, policy oversight, and funding prioritization. In my role as Deputy Commander of USINDOPACOM, I have participated first-hand in positive interactions with the Senate Armed Services Committee (SASC) and Congress to communicate on the most difficult challenges, including the pacing threat to our nation. Members of the SASC conduct a variety of engagements, including office calls, briefings, and delegation visits to exercise their oversight functions. If confirmed, I am committed to continuing a collaborative relationship with SASC and

Congress as the USCYBERCOM Commander and to ensure timely and responsive communication on cyber matters.

13. If confirmed, what actions would you take to sustain a productive and mutually beneficial relationship between Congress and U.S. Cyber Command?

If confirmed, I would ensure a strong dialogue exists between Congress and USCYBERCOM and look forward to building an engaged partnership. I will ensure compliance with relevant statues, including provisions of the annual National Defense Authorization Act (NDAA), and other relevant laws. I will build upon close relationships with members of the SASC and other congressional defense oversight committees, ensuring my Legislative Liaison office continues to work closely with the PSMs and personal staff members.

Cyber Threats

14. In your view, what are the most serious cyber threats facing the United States today, and what potential targets are the most vulnerable or susceptible to cyber attacks?

The United States faces a complex and multi-layered cyber threat landscape, but there is no ambiguity about our primary threat—China is the most serious and sophisticated threat we face in cyberspace. China's cyber forces are well-resourced, highly skilled, and tightly integrated with Beijing’s national and military objectives. Their clear intention is to challenge U.S. interests by penetrating our most critical systems, including our nation’s critical infrastructure systems. Simultaneously, there are numerous threats to our nation’s security posed by Russia, Iran, North Korea and by violent extremists, transnational criminal organizations, and other non-state actors.

15. What future strategic cyber threats and potential targets should the United States prepare for?

The United States must accelerate efforts to thwart the strategic effort by global adversaries to pre-position malicious capabilities to attack our nation's critical infrastructure and civilian targets. The threat posed by the placement of tools to attack essential services in the United States and the U.S. economy threatens stability and carries the unacceptable risk of causing civilian casualties, both in a potential conflict and in peacetime if left undefended. In the future, these actors will continually leverage cyberspace for espionage disinformation, and to enhance non-kinetic and kinetic effects.

16. In your view, how have the threats in cyberspace evolved over the past decade?

Over the last decade the evolution of threats in cyberspace represents one of the most significant shifts in modern warfare and national security. The tactics have become stealthier, and the barrier to entry has lowered. The change has been dramatic, moving from what was primarily a challenge of espionage and theft to a direct threat to our way of life.

A decade ago, the primary threat we faced in this domain was theft of information to gain an economic or intelligence advantage. Today, our adversaries have fully integrated cyber operations into their military doctrine and national strategy. Their intent is to be able to hold our critical infrastructure at risk—our power grids, financial systems, communication networks, and other civilian infrastructure—and to use that leverage to deter us in a crisis or cripple our response in a conflict. Additionally, a variety of non-state actors employ offensive cyber capabilities that threaten the security of the U.S. homeland.

17. **What are your views on the cyber capabilities and intentions of the People's Republic of China, especially regarding potential cyber attacks on U.S. critical infrastructure prior to and during any possible military operations against Taiwan?**

The cyber capabilities and intentions of the China is the most significant cyber threat to the United States. The speed at which China is advancing in critical technologies is unprecedented, and they've accomplished their technological advancement through massive state investment, systematic intellectual property theft, and the exploitation of open academic and commercial collaboration. This presents serious risks in peacetime and in the event of a conflict.

18. **What are your views on North Korea's cyber capabilities?**

North Korea's cyber program poses a sophisticated threat to the United States and our allies. North Korean state actors conduct malicious cyber activity to collect intelligence, compromise critical infrastructure, and to generate illicit revenue to evade sanctions. At USINDOPACOM, we are increasingly concerned with North Korea's theft of cryptocurrency to generate revenue for Kim Jong Un's regime's effort to expand North Korea's long-range missile capabilities.

19. **What are your views on Iran's cyber capabilities?**

Iran's growing expertise and demonstrated willingness to conduct aggressive cyberspace operations makes it a major threat to U.S. and partner network data. It is my understanding that Iran considers its cyber program as an important tool to retaliate and gather intelligence against adversaries. Domestically, Iran uses its cyber capacities to help control its population.

20. **What are your views on transnational terrorist groups' and transnational criminal organizations' cyber capabilities? In particular, do you believe U.S. Cyber Command should have a role in assessing and undermining these capabilities?**

Transnational terrorist groups primarily leverage cyberspace to conduct activities in support of their kinetic operations. They use cyberspace for secure communications, recruitment, financial transactions, media and propaganda, and research. Foreign terrorist groups have limited offensive cyber capabilities, and those they do have are largely unsophisticated and limited to website defacements. Transnational criminal organizations (TCOs) facilitate the flow of illicit drugs, including fentanyl, into the United States. These TCOs are sophisticated and possess notable capability, capacity, and resources. USCYBERCOM works closely with the other combatant commands on transnational issues.

U.S. Cyber Command Missions

21. In a strategic sense, how do you define the U.S. Cyber Command mission?

Consistent with Title 10, U.S.C. Section §167b, the principal mission of USCYBERCOM is to direct, synchronize, and coordinate military cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners. USCYBERCOM also has Unified Command Plan responsibilities for: planning and executing cyberspace operations, as directed, the Cyberspace Operations Joint Force Provider, and the Joint Cyberspace Trainer.

22. How do you define the role of the Cyber National Mission Force in countering adversary cyber forces in the event that such forces undertake destructive or obstructive attacks on the United States?

The Cyber National Mission Force (CNMF) is the U.S. military’s cyber force specifically organized, trained, and equipped to defend the nation in cyberspace. In the event of a destructive or obstructive attack on the homeland, the CNMF's mission is to execute the full spectrum of cyberspace operations to counter that adversary. This means tracking them, evicting them from our networks, and, when directed by the President, imposing costs to make them cease their malicious activity. Ultimately, the CNMF is the force we task to defeat significant adversary cyber operations, ensuring the defense of our nation in this critical warfighting domain.

23. In your view, how do you believe the existing command and control relationships between U.S. Cyber Command and the geographic combatant commands can be improved to provide the required integration in both planning and execution for contingencies, conflicts, and crisis?

The existing command and control relationships between USCYBERCOM and the geographic combatant commands are strong and encourage operational collaboration. In my current role as Deputy Commander, USINDOPACOM, I have seen first-hand how the integration of USCYBERCOM with the geographic combatant command provides the full spectrum of national power. Existing Cyberspace Operations-Integrated Planning Elements (CO-IPE) consist of USCYBERCOM representatives who are directly embedded into the geographic combatant command staffs. They work side-by-side with the air, space, maritime, and land component planners to develop all-domain solutions from the outset and are seamlessly integrated to give decisionmakers more options and ensure mission success. If confirmed, I look forward to continuing to support this model.

24. If confirmed, what steps will you take to ensure U.S. Cyber Command is successfully integrating its defensive, offensive, and command support missions within critical kill chains of the non-cyber operational components of the Department of Defense?

USCYBERCOM's successful integration of its defensive, offensive, and command support missions is essential to enabling the Department's operational kill chains. Our defensive operations ensure the integrity of friendly operational networks, while our offensive capabilities are synchronized to deliver non-kinetic effects against adversary systems. This is achieved through the direct support of our CO-IPEs embedded within the combatant commands, and the general support assignment of the Joint Force Headquarters-Cyber (JFHQ-C) components.

25. What organizational and authorities challenges remain at U.S. Cyber Command related to its missions? Specifically, do you think that additional organizational changes and authorities will be needed to resolve the readiness problem within the Cyber Mission Force?

It is my understanding that Congress and the Department have provided significant authorities to enhance the CMF. USCYBERCOM's Enhanced Budgetary Control, expanded role in setting standards for joint training and acquisition, and the Cyber Excepted Service for civilian talent are the core mechanisms that allow USCYBERCOM to align its priorities and execute more effectively. If confirmed, I will continuously assess if this powerful toolkit is sufficient and agile enough to outpace our pacing threat and to generate the world's most dominant and ready cyber force.

26. What role do you see expeditionary, or tactical, cyber playing in future conflict, crisis, and contingencies? In your view, what is the needed command and control of those organizations with respect to U.S. Cyber Command?

This is a critical area of development for the joint force. My recent command experiences in the U.S. Indo-Pacific Area of Responsibility (AOR) have given me first-hand knowledge of the command and control structures required for effective expeditionary cyber activities. In my view, we must empower the commander at the tactical edge to integrate cyber as a direct warfighting tool at the lowest possible level. The command and control model must balance tactical agility with strategic oversight. It is my understanding that USCYBERCOM's role is to recruit, train, certify, and equip expeditionary cyber teams to a common, exacting standard. Once these teams deploy, they fall under the tactical control of the geographic or joint task force commander they are assigned to support, who is in the best position to understand the immediate battlespace and integrate a tactical cyber effect into their kill chain at the speed of relevance. If confirmed, I would work to ensure that these teams are not just deployed, but truly integrated, and that the combatant commander has the confidence to employ them as readily as they would any other warfighting asset.

27. If confirmed, would you recommend or support any changes in the missions currently assigned to U.S. Cyber Command given that some experts have recommended that U.S. Cyber Command assume responsibility for additional elements of information warfare, including information operations and electromagnetic spectrum operations? If so, what changes would you recommend?

I don’t recommend changes to the current missions assigned at this time. USCYBERCOM has an important role to play in cyber-enabled information activities, but I believe it is best done in partnership with the other combatant commands. If confirmed, this will be an area that I will review closely with the Joint Staff, USSOCOM, the geographic combatant commands, and the Services and in consultation with Secretary and Deputy Secretary.

28. Do you agree with former CYBERCOM Commander General Nakasone that election security and defending the United States from foreign influence campaigns were “no fail” missions of both the NSA and U.S. Cyber Command? Please explain your answer. If possible, give some examples of how we are better positioned to defend against such attacks today than we were prior to 2016.

Any foreign attempt to undermine the American public's faith in our democratic process is a direct attack on the foundation of our nation and a core national security imperative. We are far better positioned to defend this process today primarily because we have shifted from a reactive stance to a proactive one built on partnership. The establishment of the Election Security Group, which fuses our efforts with interagency partners, allows us to rapidly share threat intelligence. Through USCYBERCOM’s "Defend Forward" posture, it is my understanding that the Command now hunts for adversaries on foreign networks and works to impose costs before their malign influence campaigns can reach the American people. This proactive, integrated effort is the key difference between our posture today and that of 2016. Efforts to counter foreign actors must be conducted carefully and only foreign-focused, and with full transparency.

National Security Agency (NSA) Missions

29. What is your understanding of the NSA mission?

It is my understanding that NSA has two missions, SIGINT and Cybersecurity. NSA collects and produces SIGINT information for foreign intelligence and counterintelligence purposes to support national and departmental missions, including crucial SIGINT support for the conduct of military operations while protecting the civil liberties and rights of U.S. persons. NSA’s Cybersecurity mission prevents and eradicates threats to U.S. national security systems, with an initial focus on the Defense Industrial Base (DIB) and improving our nation’s weapons’ security.

30. What is your understanding of the NSA mission as it relates to cyber?

As the National Manager for National Security Systems (NSS), it is my understanding that NSA is the U.S. Government focal point for cryptography, and information systems security for NSS. In this role, NSA prevents and eradicates threats to these systems, including by examining U.S. Government national security systems and evaluating their vulnerability to foreign interception and exploitation. NSA also provides critical threat intelligence on foreign cyber threats to those national security systems.

31. In your view, what role should the NSA play in support of U.S. Cyber Command and does it differ from the support that the NSA provides to other combatant commands?

As a U.S. Intelligence Community element and a Combat Support Agency (CSA), NSA plays a crucial role in generating insightful, timely, and relevant intelligence that supports operational commands, to include USCYBERCOM. NSA's SIGINT mission and its role in cybersecurity complement USCYBERCOM's role in cyberspace operations, providing unique opportunities to support USCYBERCOM.

32. Do you believe that any of the mass or narrow surveillance capabilities currently employed by the NSA should be reconsidered or adjusted?

If confirmed as the Director of NSA, I will diligently review NSA collection capabilities and operations. I am committed to exploring areas for potential improvement and, where necessary, will consider adjustments to enhance NSA's ability to protect national security while protecting Americans' privacy and civil liberties through compliance and oversight.

<u>Section 702 of the Foreign Intelligence Surveillance Act</u>

Section 702 of the Foreign Intelligence Surveillance Act will expire on April 20, 2026, unless renewed by Congress. There is bipartisan concern that queries of data collected under 702 using U.S. Persons search terms are conducted without a probable cause-based court order.

33. In your view, what is the continuing value of section 702 collection?

As a current customer of FISA Section 702 derived intelligence products, I recognize how this authority is used every day to protect the nation from current and emerging threats by providing critical insights on key adversaries. However, I would defer to the Administration to fully characterize the value of this authority. If confirmed, I fully commit to working with Congress on all matters related to this authority.

34. What is your understanding of the guardrails and processes in place to ensure that this authority is executed within current statutory guidelines and to protect U.S. citizens from the possible abuse of this authority?

It is my understanding that NSA has invested immense effort and resources to ensure the compliance process is robust and thorough, reflecting an unwavering commitment to protecting Americans' privacy and civil liberties. However, I have limited familiarity with the details of these processes in my current role with USINDOPACOM. If confirmed, I am committed to ensuring NSA executes the authority effectively and in accordance with the law.

35. If section 702 were to be extended without limiting the authority to query the data using U.S. Persons' identifiers or search terms, how do you think that would impact the NSA's mission?

This is an issue I have limited familiarity within my current role with USINDOPACOM. At this time, I defer to NSA leadership to fully characterize the existing efforts taking place under this authority. If confirmed, I fully commit to working with Congress on all matters related to this authority.

36. If the 702 database is queried using U.S. Persons identifiers for the positive purpose of victim notification, in your view, is it feasible to construct a set of rules that would permit such searches while requiring a court order for criminal or intelligence investigations? How do you think that would impact NSA's mission?

In my current role with USINDOPACOM, I have limited familiarity with this topic. If confirmed, I will be in a better position to consider the specifics of NSA's Section 702 compliance and oversight systems and processes. I fully commit to working with Congress on all matters related to this authority.

37. What is your understanding of the Attorney General-approved guidelines pursuant to Executive Order 12333 for the government to query data that NSA has collected outside the United States using U.S. Persons identifiers or search terms without reaching the probable cause standard?

From my current vantage point at USINDOPACOM, this is an aspect of policy I have limited fidelity on. If confirmed, I am committed to ensuring that NSA executes this authority effectively and in accordance with the law.

Combat Support Agency

38. What is your understanding of the role of a combat support agency?

As a combat support agency, it is my understanding that NSA provides intelligence support to military operations through its SIGINT activities, while the NSA's cybersecurity personnel, products, and services ensure that military communications and data remain secure.

39. If confirmed, how would you delineate the roles and activities of the NSA as a combat support agency in support of U.S. Cyber Command versus the support provided to U.S. Cyber Command as a cyberspace domain partner under the dual-hat arrangement?

If confirmed, I will ensure that both NSA and USCYBERCOM maintain a clear understanding and respect for each other's distinct roles, resources, authorities, and responsibilities. I will ensure that agreements delineating these responsibilities and the support provided to each organization are followed and enforced.

Under the Goldwater-Nichols Act, the Chairman of the Joint Chiefs of Staff is required to regularly conduct assessments of the readiness of combat support agencies to

support the combatant commands.

40. What is your understanding of how the NSA has performed in these assessments?

In my current capacity I do not have insight into NSA's performance in these assessments. If confirmed, I will review the CJCS assessment of NSA and work to resolve any identified deficiencies in NSA support to the Combatant Commands.

41. What, if any, changes would you make as Director of NSA, if confirmed, to strengthen this support to meet the demand of future threats across all warfighting domains?

In my current role as the Deputy Commander for USINDOPACOM, I am keenly aware of the highly dynamic and complex threats facing our nation. With that experience in mind, if confirmed, I will undertake a comprehensive review of the Agency's operations, capabilities, and support structures across all domains. I am committed to ensuring that the NSA remains at the forefront of technology and intelligence to support and protect our national interests.

Act of War in Cyberspace

42. In general, what do you believe would constitute an act of war in cyberspace?

U.S. law and policy is generally clear that cyber operations causing effects comparable to a traditional armed attack—such as significant death, injury, or physical destruction—could be considered a use of force and trigger a nation's inherent right of self-defense. This may include consideration and determination of attacks that threaten the strategic stability of the United States. Ultimately, the characterization of any act and the decision to respond in self-defense is a determination for our civilian leadership. None of the traditional calculus for evaluating what constitutes an act of war changes by virtue of an action taking place in cyberspace.

43. Do you believe that current U.S. government policy provides adequate guidance and decision space for making a determination of what types of actions might constitute an act of war in cyberspace?

Yes, U.S. government policy provides a sound framework to advise civilian leadership on whether a malicious cyber attack—either by itself or combined with other hostile acts— constitutes an act of war. The pace of technological change and our adversaries' actions demand that our policies serve as living frameworks to ensure we provide the best range of military options.

44. Concerning acts of aggression in cyberspace, do you believe the Department of Defense has a comprehensive understanding of the actions that may constitute a hostile act under the Law of Armed Conflict, particularly as it relates to U. S. critical infrastructure, and the energy, transportation, power, and financial sectors within the U.S.?

NSA and USCYBERCOM work proactively alongside our partners—in the interagency, the Intelligence Community, with our allies, and critically, with the private sector who largely own and operate this infrastructure— to assess the scale and severity of aggressive acts in cyberspace and advise U.S. government leadership on proportional, military response options. Paired with the Department of War's own expertise, our partnerships across the public and private sector can help us understand the threat capabilities, intent, and vulnerabilities of our adversaries, allowing us to deter, expose, and counter malicious activity before it rises to the level of a hostile act.

Deterrence in Cyber Space

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. The Defense Science Board (DSB) Task Force report on Cyber Deterrence, issued in February 2017, concluded that it is critical for the Department of War to develop cost-imposing deterrence options based on scalable offensive cyber capabilities to hold at risk a range of assets that the leaders of strategic adversaries value most highly. The DSB report urged the Secretary of War to develop "a policy framework for cyber deterrence including: updated declaratory policy relating to U.S. responses to cyber attack and use of offensive cyber capabilities, guidance for the employment of offensive cyber, a public affairs plan, and an engagement plan for adversaries and allies."

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

Effective cyber deterrence relies on a strategy of denial, resilience, and credible response. My approach to cyber deterrence centers on three pillars: denying the enemy success; ensuring our own resilience; and having credible options to respond. The Department's strategic approach of *persistent engagement* recognizes that denying adversary footholds into U.S. systems and networks requires constant and continual contact with the adversary. Eroding adversary postured cyber intrusions removes technical options and corrodes adversary decision maker confidence that their cyber weapons will be available should they try to employ them. If confirmed, I will work to equip the Department with the offensive and defensive tools necessary to deter our adversaries. Should deterrence fail, we must be prepared to respond decisively and aggressively. To achieve this, I will review our existing capabilities, integrate military cyber operations with all other tools of national power, and work to restore deterrence in the cyber domain, if confirmed.

46. **Do you believe it is important to adopt and articulate a strategy that imposes costs based on credible options for responding against targets that adversaries' value with offensive cyber operations to cyber attacks against U.S. critical infrastructure?**

Yes. Deterrence through strength requires that we provide our civilian leadership with a full spectrum of options, including potent offensive cyber capabilities. This strategy is essential for shaping an adversary's behavior and ensuring strategic stability.

47. What is your assessment on whether the People's Republic of China is currently deterred from conducting cyber attacks against U.S. critical infrastructure?

In my assessment, China understands that a catastrophic cyber attack against our critical infrastructure in peacetime would provoke an overwhelming response from the United States. However, we recognize strong cyber defenses are not sufficient on their own to deter our adversaries. We must account China's history of cyber espionage, intellectual property theft, and information warfare as we consider our approach to deterrence in cyberspace. Cyber effects must be layered across all domains in order to provide options to best deter.

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

Cyber attacks pose a direct threat to our national security and economic vitality. If confirmed, my mission will be to execute a strategy of deterrence through a combination of denial, resilience, and credible response options. If confirmed, I will review and integrate our military cyber capabilities with all instruments of national power to defend the nation, enable the Joint Force in a contested environment, and ensure our adversaries understand the consequences of their actions.

49. For deterrence to be credible, adversaries must have some awareness regarding the capabilities they know or suspect the U.S. has. 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?

If confirmed, I would focus on ensuring the United States has the right cyber capabilities to integrate with the Joint Force to provide credible options for our civilian leaders to reveal or conceal as necessary to affect the desired policy outcomes. I will provide my best military advice on the options available, recommendation for employment, and the risk associated with each.

50. What role should perception management or even deception capabilities play in those decisions?

Shaping our adversary's perception is fundamental to deterrence. If confirmed, I will conduct a review of our cyber capabilities in this arena. My aim is to ensure USCYBERCOM can provide a full spectrum of credible options for our civilian leaders to use in managing those perceptions and strengthening deterrence.

51. In your view, how effective is U.S. Cyber Command's current deterrence posture, and are there areas for improvement?

If confirmed, I look forward to a thorough assessment of the effectiveness of USCYBERCOM's current deterrence posture. As recently demonstrated, USCYBERCOM has incredible talent and capabilities but the relentless pursuit of excellence requires regular assessment and persistent improvement.

52. In your view, are there capabilities resident in the other combatant commands that should be more closely integrated with CYBERCOM capabilities to improve our overall deterrence posture?

USCYBERCOM should be thoroughly integrated with all other combatant commands to provide the best options for layered effects to support our Joint Force warfighters. Providing credible warfighting capabilities across all domains is the best way to improve our overall deterrence posture. Working with U.S. Space Command (USSPACECOM) to layer space and cyber is one example that will be key to this.

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

As our national strategies make clear, deterrence is a team effort. Cooperation with our allies in cyberspace is critical for sharing intelligence, building advanced capabilities, and securing our networks. If confirmed, I will prioritize strengthening these partnerships to ensure we have the collective power to deter and defeat emerging threats.

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

Our adversaries don't operate in silos, and neither can we. The intersection of space, cyber, and nuclear capabilities creates complex escalation risks that demand a truly integrated approach to deterrence. If confirmed, one of my highest priorities will be to partner my fellow Combatant Commanders, particularly with the Commanders of U.S. Space Command and U.S. Strategic Command to ensure our planning, capabilities, and operations are fully synchronized. The goal is to deliver seamless, multi-domain options to our civilian leaders – options that complicate an adversary's calculus, reinforce deterrence, and should it fail, maximize the lethality of the Joint Force.

55. 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?

For the defense of the homeland, USNORTHCOM is the supported combatant commander, and USCYBERCOM is a critical supporting command. This relationship is fundamental to our national security, especially in countering foreign malicious actors—like cartels or state-sponsored groups—that use cyberspace to threaten our homeland security, including at the southern border. While USCYBERCOM's primary mission is defending the homeland from foreign threats, its capabilities can provide limited, appropriate support to civil authorities under USNORTHCOM's lead when directed. My commitment is to ensure this partnership is rock-solid, delivering a unified defense against the nation's most pressing threats.

Department of Defense's Role in Defending the Nation from Cyber Attack

56. What is your understanding of the role of the Department of Defense in

defending the Nation from an attack in cyberspace? In what ways is this role distinct from those of the homeland security and law enforcement communities?

The Department's role is to defend the nation from foreign cyber threats by employing the military instrument of power abroad. Our primary strategy has been to defend forward, which is a proactive, three-part operation:

1. **Generate Insight**: To actively hunt for adversary activity in foreign cyberspace to understand their tools, tactics, and intentions.
2. **Enable Partners: S**hare this vital intelligence with our federal, state, local, and international partners, allowing them to harden their own defenses.
3. **Impose Costs:** When necessary and authorized, take direct action against foreign adversaries to disrupt their operations before they can harm the United States.

Separately, in the event of a significant domestic cyber incident that overwhelms the capacity of another agency like DHS, the Department can provide Defense Support of Civil Authorities upon request. It is important to clarify that the Department defers to DHS, the Department of Justice the Federal Bureau of Investigation and other domestically focused agencies for law enforcement and homeland security matters.

57. What is your understanding of the specific role of the Cyber National Mission Force in disrupting cyber attacks on U.S. critical infrastructure and other non-military targets?

The CNMF operates on the principle that the best defense is to proactively engage adversaries on foreign territory. Through Hunt Forward operations (HFOs), the CNMF embeds cyber operators with key partners to hunt for malicious actors on their networks. This allows the CNMF to observe adversary Tactics, Techniques, and Procedures (TTPs) before they arrive at our doorstep. These forward deployments provide a triple dividend: they enable direct disruption of adversary campaigns, they help the United States build trust with our allies and partners, and they provide insight on emerging threats. The CNMF then channels intelligence gathered through HFOs back to our partners at DHS and the FBI, as well as to industry, directly strengthening our collective homeland defense.

58. Can you describe how a request for Defense Support to Civil Authorities (DSCA) by appropriate civilian leadership might be made in the event of a cyber incident? Are those processes trained for and exercised with U.S. Cyber Command, and the inter-agency community?

The Defense Support of Civil Authorities, or DSCA, process is the well-established framework for providing military assistance in a domestic crisis. In the event of a significant cyber incident, a request from a lead federal agency, like DHS or the FBI, would be made to the Department for unique capabilities. I understand that this is not just a plan on a shelf; it is a muscle exercised regularly as USCYBERCOM works shoulder-to-shoulder with partners at DHS, CISA, the FBI, USNORTHCOM, and private industry. The goal is to ensure seamless coordination and shared situational awareness, so if a request comes, we are ready to respond at speed.

59. In your view, does U.S. Cyber Command have the capacity and the authority to directly operate in the networks of domestic critical infrastructure providers to defend against major cyber attacks?

It is important to understand that the majority of the United States critical infrastructure is owned and operated by the private sector. Furthermore, USCYBERCOM's mission is to defend the nation against adversaries in cyberspace. It is my understanding that the command is legally and operationally precluded from conducting domestic missions, instead functioning as an enabler for domestic partners like the DHS and FBI. In crisis, USCYBERCOM could bring critical capabilities to support a domestic response under the DSCA framework. When directed, USCYBERCOM can support civil authorities in defending U.S. critical infrastructure from malicious cyber activities, a role it would perform in coordination with and in support of the homeland defense missions of USNORTHCOM and/or USINDOPACOM.

60. What is your understanding of the expected role of the National Guard and the reserve component in defending critical infrastructure from cyber attacks in support of civil authorities?

Members of the National Guard enhance USCYBERCOM's missions and provide essential cyber capabilities to their home states. Many Guard members bring valuable private-sector experience, allowing them to quickly share threat information with state and local authorities. They can operate under state authority (Title 32) to protect critical infrastructure or be federally mobilized under Title 10 to directly support USCYBERCOM's national mission.

61. What is your understanding of the government's policies in recognizing and responding to cyberspace gray zone activities below the threshold of war in which cyber attacks might be used against U.S. homeland critical infrastructure and military assets worldwide to deter U.S. military action by impeding U.S. decision making, inducing societal panic, and interfering with the deployment of U.S. forces?

The United States employs all aspects of its national power to combat cyber threats from foreign adversaries. The executive branch is focused on protecting critical infrastructure and national security systems. The Department is authorized to conduct military operations in foreign cyberspace to disrupt and defend against malicious cyber activities targeting the U.S. government, its people, and critical infrastructure. This approach has improved the Department's ability to recognize and mitigate these threats in collaboration with domestic and international partners.

Dual Hat

62. Do you believe that the dual hat arrangement should be maintained?

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 USCYBERCOM 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. From my perspective as the Deputy Commander of a geographic combatant command, the ability to fuse intelligence and operations at speed is a decisive advantage. I understand the Dual Hat Study led by General Dunford affirmed that this arrangement is in the best interest of the nation. The missions are inextricably linked, and if confirmed, I would be committed to ensuring the unity of effort that this arrangement provides continues to deliver results for the Joint Force, while continuing to assess if this is the most effective way to support the warfighter.

63. In your view, are the demands of both commanding U.S. Cyber Command and directing the NSA overly stressing for a single official?

I have no doubt the demands of both roles are significant. However, my understanding is that the structure is designed to support a single commander, with robust senior leadership teams in place at both organizations to manage day-to-day operations. The role of the commander is to provide unified strategic direction. If confirmed, I would consider these and other factors in any assessment that I conduct regarding the dual hat.

64. In your view, would it be as time-consuming and complex for separate NSA Directors and Commanders of U.S. Cyber Command to coordinate and integrate their mission sets and capabilities?

From an operational perspective, creating two separate leaders for two deeply intertwined missions could add time and complexity. It could require deconfliction and negotiation for issues that are currently resolved under a single commander. In a domain where speed is paramount, adding bureaucracy would create risk and cede the advantage to our adversaries. If confirmed, I will continue to assess this.

65. If confirmed, what are your views on NSA’s budgets and personnel subsidizing U.S. Cyber Command and the non-National Intelligence Program budget of the DOD?

If confirmed, I would operate on the clear principle that all funds must be used for their congressionally appropriated purpose. While I am not familiar with the specific accounting details today, I understand that the Joint Study confirmed that clear processes are now in place to ensure accountability and cost reimbursement between the two organizations. Enforcing those agreements rigorously would be a key priority for me.

66. If confirmed, what are your views on U.S. Cyber Command often gaining accesses to targets from the NSA for military purposes that negates their significant value for NSA’s national intelligence mission?

My understanding is that this "gain/loss" decision is one of the most critical responsibilities of the dual-hatted commander. If confirmed, my approach would be to ensure that the process for making these decisions is rigorous and that the risks to intelligence collection are fully weighed against the potential operational benefits. As the single individual accountable for both mission outcomes, I would provide our nation’s leaders with informed options that preserve their decision advantage, if confirmed.

67. If confirmed, what are your views on U.S. Cyber Command preparing for or undertaking operations against targets due to objections that such actions would jeopardize intelligence collection? What are your views of such tradeoffs?

I view these tradeoffs as one of the principal values of the dual-hat arrangement. It is not about one organization winning an argument over the other; it is about a single leader making an informed risk decision on behalf of the nation. A leader who is accountable to both the Secretary and the DNI is uniquely positioned to make that call. If confirmed, I would rely on the experts at both NSA and USCYBERCOM to provide their best assessments to inform these critical decisions.

68. In your view, is the degree of support that U.S. Cyber Command receives from the NSA detrimental to the support that NSA provides to other combatant commands and to national policymakers?

As the Deputy Commander of USINDOPACOM, I have been a major customer of NSA's combat support, and it has been excellent. I have not seen any indication that support to other combatant commands has been degraded. If confirmed, I would be accountable for ensuring the NSA continues to provide world-class support to the entire Joint Force and our national leadership, not just one command.

Cryptographic Modernization

In fiscal year 2022, the Joint Staff Director for Command, Control, Communications and Computers (C4)/Cyber, and the Chief Information Officer refused to continue issuing waivers for cryptographic systems that the NSA had determined were obsolete, vulnerable and should be replaced.

69. What is your understanding of the problems in the overall cryptographic modernization program?

I believe we must have strong and secure cryptographic capabilities, and if confirmed, I will assess the state of those capabilities. I am also aware of the threat posed by the potential future development of a powerful quantum computer in adversary hands that could break public-key cryptosystems used within the United States and around the world. Modernization efforts should be focused on ensuring that the Department’s cryptography is strong and secure not only today but also–ensuring that the Department’s cryptographic inventory is modernized to be completely quantum resistant.

70. In your view, has the Department of Defense made significant changes in the way that cryptographic modernization is overseen and managed that make that program more effective? Please explain your answer.

I believe that successful modernization requires continued, significant interagency coordination as well as alignment of budgetary and technical resources needed to accomplish the goal. If confirmed, I look forward to making an assessment and the Department manages cryptographic modernization.

71. If confirmed, what are your views on the pace of progress in developing and deploying quantum-resistant cryptographic solutions in the Department of Defense, in National Security Systems across the government, and in the private sector, as compared to the pace of progress of the development of quantum computers that would be able to break public key encryption?

I understand that NSM-10 sets a target for the Federal Government to achieve full post-quantum cryptographic modernization by 2035. This is a challenging, yet attainable, goal. I understand that annually, NSA and the military departments release cryptographic modernization roadmaps. If confirmed, I would conduct an assessment to understand NSA's ability to execute these roadmaps.

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."

72. **In your view, what progress have services made so far to achieve the necessary levels of personnel readiness in the Cyber Mission Force (CMF)? What is still needed?**

The Services face challenges in training and retaining highly skilled personnel for the CMF. I understand the Department and the Services have already made significant progress to improve the readiness of our CMF. If confirmed, I look forward to working with the Assistant Secretary for Cyber Policy/Principal Cyber Advisor, the Services, other Department stakeholders, and industry to leverage best practices to continue to improve training and retention and to sustain the required readiness that achieves domain mastery within the CMF. It is imperative that the Command continuously assesses this issue.

73. If confirmed, what 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?

The Department recently established a revised USCYBERCOM cyber force generation model to fundamentally change how USCYBERCOM recruits, assesses, trains, and retains cyber forces. This model integrates USCYBERCOM directly with the Military Departments to streamline personnel processes. This includes targeted recruiting, tailored assignment management, and optimized unit phasing. If confirmed, I will leverage existing Service readiness tools to gain a unified, Department-wide insight into our cyber force readiness.

74. 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?

If confirmed, I will work with the Assistant Secretary for Cyber Policy/Principal Cyber Advisor, the Services, and cyber service components to implement the revised cyber force generation model to ensure the Services provide the necessary, highly skilled personnel to the CMF. The goal of the cyber force generation model is to develop increased lethality, domain mastery, and mission agility in our cyber forces, ensuring they are optimized to defeat threats posed by China in cyberspace. The revised cyber force generation model will continuously build a future cyber force capable of defeating the most significant threats in cyberspace and delivering asymmetric options to the Joint Force.

Acquisition and Development of Cyber Capabilities

75. In your view, what progress has CYBERCOM made in maturing their own organic capability development? What areas are still needed for improvement?

Congress has provided Service-like authorities and enhanced budget control (EBC) to USCYBERCOM in order to improve the pace and scale of organic cyber capability development. Leveraging these tools, USCYBERCOM can continue to accelerate speed of development and acquisition, capability integration into the broader joint force, and the integration of AI and machine learning into capability development. If confirmed, my focus will be on ensuring our organic capability development delivers a decisive advantage in cyberspace.

76. 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?

Private industry is a foundational strategic partner, providing the critical technology and talent that gives us our decisive military advantage. My experience in both Special Operations and at USINDOPACOM proved this partnership is essential for enhancing both our warfighting capabilities and our workforce development. I concur with the Secretary's assessment that we must move faster on acquisition, leveraging all industry partners from the largest performers to the most innovative startups. If confirmed, I will assess what necessary structural and cultural improvements need to be made to ensure the ingenuity of our private sector becomes a strategic advantage our adversaries cannot match.

Congress transferred responsibility for acquiring the Joint Cyber Warfighting Architecture (JCWA) from military department executive agents in the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117-263).

77. In your view, is it critical to the success of the JCWA initiative that the military services sustain support for the JCWA programs until U.S. Cyber Command has acquired the workforce and acquisition expertise necessary to manage and integrate these programs effectively?

It is my understanding that the Joint Cyber Warfighting Architecture (JCWA) is crucial for rapidly adopting, maturing, and transitioning innovative cyber technologies into operational capabilities. The implementation of USCYBERCOM’s revised cyber force generation model will align with and optimize resource delivery for the JCWA. If confirmed, I will work with the Office of the Under Secretary for Acquisition and Sustainment and the Assistant Secretary for Cyber Policy/Principal Cyber Advisor to advance the JCWA’s development.

78. What is your understanding of the military services commitment to providing that support until a suitable transition can be planned?

I understand that the Services are fully committed to providing the necessary personnel and resources to sustain our cyber operations until the Joint Cyber Warfighting Architecture achieves full operational capability. If confirmed, I will work in close partnership with them to evaluate the plan for a suitable transition that ensures there is no degradation of our warfighting readiness.

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

Any adaptation of USCYBERCOM’s cyber force structure must directly accelerate and optimize the development of the Joint Cyber Warfighting Architecture. I understand that the USCYBERCOM revised cyber force generation model is specifically designed to do this, aligning organizational and programmatic functions to ensure USCYBERCOM delivers the right talent to build and operate the JCWA. The goal is complete integration, where the evolution of our force and our technology are inextricably linked to produce a more lethal and agile warfighting capability.

The Defense Advanced Research Projects Agency (DARPA) has volunteered, and U.S. Cyber Command accepted the offer, to provide a flow of software-based capabilities to the Command for integration into JCWA.

80. In your view, what are the important features and advantages of this initiative, both for the Command and DARPA?

It is my understanding that the initiative between DARPA and USCYBERCOM is designed to solve one of our most persistent challenges: speed. It creates a virtuous cycle by accelerating the delivery of cutting-edge tools to USCYBERCOM while ensuring DARPA's next generation of research focuses on solving our most stressing operational problems. It is a powerful model for maintaining our nation's decisive edge in cyberspace.

81. 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?

If confirmed, advocating for science and technology (S&T) resources will be a top priority. My approach will be to partner directly with the Under Secretary for Research & Engineering, the Assistant Secretary for Cyber Policy/Principal Cyber Advisor, and the Services to strongly advocate for these science and technology (S&T) investments. If confirmed, I will explore how to leverage USCYBERCOM's Enhanced Budget Control mechanisms to integrate funding and acquisition processes to support research required for future cyber capabilities.

82. 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?

The broader DOW S&T enterprise conducts the foundational, next-generation research that we cannot replicate. The promise of CYBERCOM 2.0 is that our modernized force structure and agile acquisition processes will make us a better partner to rapidly transition their vital work into the practical tools our joint warfighters need. If confirmed, my focus will be on strengthening this collaborative, department-wide effort to accelerate the fielding of these future capabilities and prevent redundancy.

In addition to U.S. Cyber Command's internal ability, including the developers and analysts in the Cyber Mission Force units, to develop tools and accesses necessary to conduct its mission, such capabilities and resources can be acquired commercially.

83. In your view, does U.S. Cyber Command have the necessary authorities and processes to acquire accesses and tools to support offensive and defensive capabilities from the private sector when the opportunity arises?

USCYBERCOM possesses substantial authorities, but the true challenge lies in the agility of our processes. From my experience, speed is decisive. If confirmed, I will work to ensure we are always postured to rapidly field the most advanced commercial capabilities to our cyber operators.

84. Does the Department possess the requisite relationships with private sector entities and vendors to rapidly acquire cyber capabilities? If not, what recommendations would you make to build those relationships?

Drawing from my experience in the U.S. Special Operations community, I understand the importance of establishing the critical private-sector relationships needed to acquire capabilities at a tempo that supports our operations. My experience has taught me that we can gain an even greater advantage by evolving these relationships from merely transactional to deeply integrated partnerships. This means embedding our operators directly with industry talent to solve our hardest problems, ensuring we outpace the speed of the threat.

Cyber Support to Geographic Combatant Commands

Section 1537 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117-263) directs the Principal Cyber Advisor of the Department of Defense to conduct a study on the support to combatant commands. This study highlighted the growing focus on verifying the correct level of integration of cyber operations into planning for contingencies as well as emerging crisis and conflicts.

85. In your view, what improvements can be made to enhance integration of cyber operations – defensive and offensive – into combatant command plans for contingencies, as well as emerging crises and conflicts?

As the Deputy Commander at USINDOPACOM, I have seen the evolution of USCYBERCOM support to the Joint Force first-hand, both in exercises and in real world operations. In my view, we must accelerate the shift in the mindset that cyber is not merely a supporting capability, but the key enabler in operations across all domains. Improved network interoperability between USCYBERCOM, the combatant commands, and our partners will provide more rapid and useful cyber effects for combatant commanders. If confirmed, I look forward to working with partners to implement the new cyber force generation model to enhance integration of full spectrum cyberspace operations into the Department's operations, from the earliest stages of planning through execution.

86. If confirmed, how will you continue to evaluate the force posture across the combatant commands?

If confirmed, I will work in direct coordination with the other combatant commands through our established force allocation and assessment processes. This approach ensures our cyber forces remain aligned against our nation's top priorities. We will use ongoing reassessments to stay agile, allowing us to rapidly address emergent requirements and the evolving cyber threat landscape.

87. What is your assessment of the operational control and oversight necessary to ensure effective cyber operations in support of combatant commanders?

USCYBERCOM must be thoroughly integrated with all other combatant commands to provide our Joint warfighters with the best options for layered effects. This coherence is the most effective way to improve our overall deterrence posture while managing risk in the globally interconnected cyber domain.

Integration of Cyber Capabilities in Multi-Domain Operations

Section 1510 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117-263) required the Secretary of Defense to establish forces, capabilities, and information support to enable the delivery of non-kinetic effects that provide increased survivability and effectiveness of engaged military forces.

88. What are your views on the potential utility of tactical cyber forces able to deliver such non-kinetic effects?

Having forces that can deliver localized, non-kinetic effects gives a combatant commander more tools in their toolkit to provide integrated effects. The ability to disrupt an adversary's command and control or targeting systems at the tactical edge—without firing a shot—can create significant advantages, shape the battlespace, and protect our forces. This is a capability that directly supports the warfighter.

89. Do you think such forces should be service-retained and controlled by the geographic combatant commands or should they be part of the Cyber Mission Force under the command of U.S. Cyber Command? Please explain your answer.

The Services should be responsible for organizing, training, and equipping these tactical forces as part of their warfighting formations. The geographic or joint task force commander must have tactical control of these assets within their area of responsibility to integrate their effects. However, USCYBERCOM must set the standards and deconflict these operations globally to prevent unintended consequences. This ensures a combatant commander has the capability they need, while the global cyberspace commander maintains overall strategic coherence.

90. In your view, do you think that cyber operations against tactical military systems will become more common in the future? If so, are we developing the technology and operational concepts needed to enable such operations at an adequate pace?

I am certain they will become more common. Our adversaries are watching how we fight, and they will seek to exploit our reliance on networked tactical systems. My primary concern is the pace at which we are developing and fielding our own capabilities. We have good ideas, but we must get the technology out of the lab and into the hands of our warfighters more quickly. If confirmed, accelerating that transition would be a key area of focus for me.

91. In your view, will this lead to a higher valuation of the cyber mission by the combatant commands and the military services?

When a tactical commander sees a cyber operation directly enable their mission—whether by protecting their network or by disrupting the enemy's—the value becomes clear and undeniable. The more USCYBERCOM demonstrates that cyber can provide a tangible advantage on the battlefield, the more it will be integrated into our core warfighting doctrine and valued by commanders across the Joint Force.

<u>Enhanced Budget Control (EBC)</u>

The National Defense Authorization Act for Fiscal Year 2022 (Public Law 117-81) included legislation that provided enhanced budget control (EBC) for the Commander of U.S. Cyber Command. This EBC authority included the ability to propose a budget for the cyber mission to the leadership of the Department of Defense.

92. In your view, what impact, if any, has the EBC authority had on the resources

allocated to the cyber mission?

It is my understanding that USCYBERCOM has seen a steady increase in resources since the department implemented enhanced budgetary control (EBC). EBC has given the commander a direct voice in the Department's budget process. I would expect this to improve force readiness and warfighting capabilities.

93. What is your understanding of the effectiveness of the transition to this new budget process?

My understanding is that the Command's transition has gone smoothly. If confirmed, I look forward to continuing to provide Congress updates on this process through annual reports and being responsive to Congressional oversight requests.

94. In your view, are there any indications that the military services will, as a result of EBC, reduce the level of support for the cyber mission in those areas where budget authority was not transferred to the Command, such as basic research and intelligence analysis?

It is my understanding that the military Services continue to sustain investments in the cyber domain.

95. What mechanisms would you have, if confirmed, to monitor and respond if the services take such action?

If confirmed, my goal will be to coordinate with the services and key Department leaders such as the Assistant Secretary for Cyber Policy/Principal Cyber Advisor and CIO to ensure our investments are synchronized. If confirmed, I would participate in a number of budgetary processes led by the Department that will afford me an opportunity to highlight if further service support to the cyber force is necessary.

Cyber Force

Since the establishment of U.S. Cyber Command in 2010, Congress and the leadership of the Department of Defense have modeled the evolution of the Command on U.S. Special Operations Command (SOCOM). However, there has been some support for creating a separate Cyber Force, partly in response to persistent readiness problems.

96. What are your views on whether DOD should continue to mature U.S. Cyber Command according to the SOCOM model or instead create a separate cyber service? Please explain your answer in detail.

From my perspective, the USSOCOM model has been a tremendous success for the nation. My understanding is that Congress has deliberately set USCYBERCOM on a similar path, providing new authorities like EBC to give the commander the tools they need.

If confirmed, my first step would be to conduct a deep assessment of how effectively those new authorities are being implemented. We need to give them time to work. Before considering a major reorganization like creating a new Service, I would want to understand the results of the ongoing studies mandated by Congress and work with this Committee to determine the best path forward for the force.

97. What are some of the potential downsides that could result from a decision to establish a separate cyber service?

If confirmed, I would want to assess whether such an effort could detract from our focus on confronting our adversaries or negatively impact readiness in the near term. These are risks that would need to be carefully weighed.

98. In your view, can DOD solve the readiness problem in the Cyber Mission Force units pursuant to legislative actions and direction from the Secretary and Deputy Secretary of Defense? Please explain your answer.

I believe the Department now has adequate authorities to address the readiness challenges. The key is execution. If confirmed, my top priority would be to work in lockstep with the Service Chiefs to implement the solutions that have been discussed, such as longer tour lengths and standardized training. I would need to look closely at the current implementation plans and, once I have a better understanding, commit to reporting back to this Committee on our progress and any roadblocks we encounter.

99. Do you think that it is necessary to enhance the authority of the Commander of U.S. Cyber Command in the area of personnel policy, training, and retention in order to ensure stability in the readiness of the Cyber Mission Force? If so, what specific steps would you recommend?

At this time, from my current position, I do not see a need for new authorities. It is my understanding that Service-like authorities that Congress recently granted to USCYBERCOM are significant. If confirmed, my immediate focus would be on fully leveraging the tools we already have. I would need to get in and assess how the Command and the Services are using these existing authorities to impact readiness. I would need to conduct that review and understand where the true gaps and friction points are before I could recommend any specific new steps or authorities.

<u>Impact of Artificial Intelligence/Machine Learning</u>

Recent advances in Artificial Intelligence (AI) promise to enable the automation of sophisticated analysis of situations and conditions, and adept control of large numbers of complex machines and operations. 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.

100. What are your views about the potential impacts of AI on the future cyber threat, the information warfare threat, and military operations in cyberspace, and when would you expect to see them?

When applied to cyber missions, AI has the potential to both enhance our ability to exploit vulnerabilities and to accelerate the speed and scale of our cyber operations. However, AI can also enable our adversaries and competitors in the same ways, as well as lower the cost of entry to others with intent to harm the United States. In my current role as Deputy Commander at USINDOPACOM, our Command focuses on leveraging AI to improve the speed and accuracy of the Commander's decision cycle. If confirmed, I will evaluate how USCYBERCOM can continue to accelerate AI adoption to negate threats and maintain decision advantage, aiming for substantial operational impacts as outlined in the USCYBERCOM AI roadmap.

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

Sustained, prioritized funding in foundational capability areas critical for AI in the cyber domain is paramount to include secure data and pathways, resilient infrastructure, Joint and Combined interoperability standards and protocols, and a skilled and appropriately AI-enabled cyber workforce ready to execute, Joint, all-domain operations. If confirmed, I will evaluate how to enhance the speed and operational impact when deploying decisive AI capabilities to the warfighter and advocate for efforts to outpace our adversaries and ensure our AI and AI-enabled workforce are superior.

102. 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?

My experience in the Special Operations community gave me first-hand experience with the Service-like authorities that are transformational for operational Commands to get critical technology to the warfighter at speed. If confirmed, I will personally evaluate USCYBERCOM's Enhanced Budget Control and unique authorities, working with the Department and the Services to shorten the timeline from identifying a requirement to fielding a capability for our cyberspace operators.

103. 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?

If confirmed, I will forge mission-driven partnerships across the Department, industry, and our allies and partners to accelerate the delivery of AI capabilities to our cyber operators. I will work closely with partners like the CDAO and DARPA to transition high-impact research into operational use, and with the Services and other key partners to build the necessary workforce structure. Ultimately, I will prioritize AI that augments human decision-making, improves speed and scale, and is demonstrably secure against emerging cyber threats.

104. In all of these cases, data sources or repositories are needed to enable these activities. In your view, what is the readiness of CYBERCOM's data holdings to take full advantage of artificial intelligence and machine learning technologies?

To take full advantage of operationalizing AI and machine learning technology, there must be optimal interoperability between data sources and repositories. If confirmed, I will evaluate how to improve USCYBERCOM's ability to query across different domains and standardize data formats, which will unlock the full potential of USCYBERCOM's data holdings for advanced AI and machine learning.

105. How would you assess the AI capabilities of U.S. adversaries and near-peer competitors?

In my current role as Deputy Commander of USINDOPACOM, I know that our adversaries and strategic competitors, particularly China, are investing enormous national resources to become global leaders in AI and are intent on applying the technology for military purposes with few legal or policy checks. We must assume they are pursuing this technology with a sense of urgency and purpose that matches or exceeds our own. This is a race, and if confirmed, ensuring our nation is postured to win would be one of my highest priorities.

Cybersecurity of the Nuclear Command, Control, and Communications Network

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

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

USCYBERCOM, DCDC, and NSA actively support the Commander, United States Strategic Command (USSTRATCOM) to defend the Nuclear Command, Control, and Communications (NC3) Enterprise. If confirmed, I will evaluate how USCYBERCOM counters malicious cyber activity targeting the NC3 Enterprise and continue to work with the NC3 community to increase the Department's cyber resilience.

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

USCYBERCOM, DCDC, and NSA will continue to play a central role in the cyber defense of the NC3 enterprise. These three organizations are three of the four members of the NC3 cross functional team focused on improving the cyber security posture and defense of the NC3 enterprise.

Force Mix of Civilian, Military, and Contractor Personnel in U.S. Cyber Command

108. In your view, describe any legal restrictions concerning whether a given position must be filled by military personnel, rather than a government civilian?

It is important to assess mission requirements, identify which functions are inherently governmental, and determine the appropriate manpower mix to maintain mission capability while ensuring policy compliance. Determinations regarding how positions must be filled are outlined in DoDI 1100.22, Policy and Procedures for Determining Workforce Mix. This Department guidance provides guidelines for determining the appropriate mix of military, civilian, and private sector support.

109. What are the legal and policy parameters surrounding the use of contractor personnel for the execution of military cyber operations?

Department policy directs that only federal military personnel conduct military operations involving the planned use of destructive capabilities, including offensive cyber capabilities. Contractor-provided services are valuable to the success of USCYBERCOM's missions. Civilian and contractor personnel may support offensive cyber operations not meeting the policy requirement above, however, contractors cannot cross the policy threshold of performing inherently governmental functions. If confirmed, I will ensure we maintain rigorous oversight so that inherently governmental functions are performed only by government personnel.

110. What do you believe is the appropriate force mix between civilian, military, and contractor personnel accounting for the mission, educational requirements, any legal restrictions, the ability to recruit and retain military personnel in this field, and career progression for cyber personnel?

In my view, USCYBERCOM will leverage the revised cyber force generation model and partnerships with the Services to meet the demands of a constantly evolving cyber domain. If confirmed, I will evaluate how to aggressively man, train, and equip the best cyber talent the nation has to offer through this model. The goal is to increase the lethality of our cyber forces and prioritize the domain mastery needed to decisively respond to any threat.

111. What recommendations might you make for policies to improve recruiting and retaining cyber military and civilian personnel to help reduce the increasing competition for these professionals with the commercial sector?

USCYBERCOM must actively leverage every authority the Command possesses—including the Cyber Excepted Service and unique personnel authorities—to recruit and retain high-demand cyber talent. If confirmed, I will direct the new Cyber Talent Management Organization under USCYBERCOM's revised force generation model to maximize these authorities and identify any gaps where we may need additional help from Congress. Ultimately, we must fight and win the war for talent across the global cyber enterprise; our mission success depends on it.

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).

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

Foundational intelligence provides the critical advantage in cyberspace, just as it does in every other warfighting domain. Development of this capability has to keep pace with operational needs. If confirmed, I will evaluate how to grow our technical analytic workforce and to best process data at speed and scale to produce the pertinent and timely intelligence our mission requires.

113. If confirmed, how will you advocate across the leadership of the Department, the Director of National Intelligence, the Under Secretary of Defense for Intelligence and Security, and the heads of the appropriate DOD components of the Intelligence Community for this requirement?

Foundational intelligence in cyberspace is critical to all USCYBERCOM missions. If confirmed, I will focus on ensuring that we meet USCYBERCOM's requirements and I will work directly with USD(I&S) and DIA to continue closing these gaps, particularly as they relate to understanding adversary order of battle, enumerating target networks, and building the analytic workforce. I will also advocate for increased investment to develop this expertise, specifically by expanding our partnerships to integrate specialized talent from industry, the military, and other sources to better execute the Command's mission in adherence to the National Security Strategy.

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.

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

Yes.

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

Yes.

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

Yes.

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

Yes.

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

Yes.

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

Yes.

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

Yes.