Advance Policy Questions for Lieutenant General Timothy D. Haugh, USAF
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, USCYBERCOM, is responsible for the planning of cyberspace missions; serving as the cyberspace operations joint force provider; and joint force trainer, as specified in the Unified Command Plan and 10 U.S.C. §167b. In coordination with mission partners, USCYBERCOM: directs Department of Defense information network (DoDIN) operations; secures and defends the DoDIN; maintains freedom of maneuver in cyberspace; executes full-spectrum military cyberspace operations; provides shared situational awareness of cyberspace operations, including indications and warning; integrates and synchronizes cyberspace operations with other Combatant Commands and other appropriate U.S. Government agencies tasked with defending our nation's interests in cyberspace; and supports civil authorities and international partners. These efforts support DoD's overall mission in cyberspace of defending the nation, supporting the Combatant Commands, and defending Department of Defense (DoD) networks.

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

Under the authority, direction, and control of the Under Secretary of Defense for Intelligence & Security (USD (I&S)) and the Director of National Intelligence (DNI), the Director of the National Security Agency (NSA) is responsible for ensuring the NSA successfully conducts two missions: signals intelligence (SIGINT), and cybersecurity. The SIGINT mission provides America's leaders with critical foreign intelligence to defend our country, save lives, and advance U.S. goals and interests. The cybersecurity mission prevents and eradicates threats to U.S. national security systems with a focus on the Defense Industrial Base, and the U.S. military's weapon systems. NSA's SIGINT and cybersecurity missions are also critical to fulfillment of NSA's combat support responsibilities.

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

I am a career intelligence officer who has served 31 years in intelligence positions in the Air Force, the Joint Force, and the Intelligence Community (IC). I have commanded intelligence units at the Squadron, Wing, and Numbered Air Force level, and served as a Senior Intelligence Officer in special operations, a combatant command, and Air Force intelligence units in garrison and deployed. Trained as a Signals Intelligence officer, I have served in many operational assignments within the joint and Air Force cyber force, and in intelligence assignments within the NSA and the Air Force's cryptologic component. In my cyber assignments, I have commanded units within the Air Force and Joint Force responsible for executing all of

USCYBERCOM's assigned missions. I have also been part of combined operations with NSA that allowed me to partner with or support NSA's Cybersecurity and SIGINT missions. I have been honored to serve with the military cyber forces and the NSA for most of my career, and have a deep appreciation for the talented professionals who execute both organizations' important missions in service of the nation.

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

Over the past 31 years, I have served in leadership positions across the Air Force, the Joint Force, and the Intelligence Community in peacetime and during conflict. I have commanded units at the Squadron, Group, Wing, Joint Task Force and Numbered Air Force levels prior to my current assignment as the Deputy Commander of US Cyber Command. My assignments, both in command and as a staff officer, have afforded me broad insight into command and leadership from the tactical to the strategic level, and provided substantial experience coordinating with senior government officials, congressional members and staff, senior military leaders, foreign partners, members of industry, and academia. Finally, I have been privileged to attend a number of schools for further professional education designed to prepare me for leadership and command at the senior levels of our armed forces.

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?

I am a firm believer in life-long learning. If confirmed, I would strengthen our relationships with industry, coalition partners, and interagency stakeholders, while learning from their perspectives and equities to enhance the effectiveness of our cyber and cryptologic efforts. Additionally, I intend to continue a program of self-study that involves regular interaction with those in academia, industry, the interagency, and select coalition partners to further my knowledge on leadership, technology, acquisition and cybersecurity.

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 of Defense 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 of Defense in coordination with the Chairman of the Joint Chiefs of Staff.

The Deputy Secretary of Defense

The Deputy Secretary of Defense performs such duties and exercises such powers prescribed by the Secretary of Defense. The Deputy Secretary of Defense will act for and exercise the powers of the Secretary of Defense when the Secretary is disabled or the office is vacant. If confirmed, I will work closely with the Deputy Secretary, as appropriate.

The Director of National Intelligence

As the head of the Intelligence Community, the Director of National Intelligence (DNI) acts is the principal advisor to the President and the National Security Council on intelligence matters pertaining to national security; and oversees and directs the implementation of the National Intelligence Program. The Director of National Intelligence coordinates national intelligence priorities and facilitates information sharing and coordination across the Intelligence Community. If confirmed, I will work closely with the Director of National Intelligence in the exercise of her authorities.

The Under Secretary of Defense for Policy

The Under Secretary of Defense for Policy (USD(P)) is the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary of Defense for matters regarding the formulation of national security and defense policy, and the integration of DoD 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 of Defense for Intelligence & Security (USD(I&S)) is the advisor and PSA to the Secretary and Deputy Secretary of Defense 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 of Defense over the National Security Agency / Central Security Service, subject to authority of the DoD Chief Information Officer concerning the activities of the Cybersecurity Directorate. 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 Under Secretary of Defense for Acquisition and Sustainment

The Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) is the PSA and advisor to the Secretary of Defense for all matters relating to acquisition and sustainment in the DoD, and serves as the senior procurement executive for the Department of Defense, 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 of Defense for Research and Engineering (USD(R&E)) is responsible for overseeing the research, engineering, and technology development activities across the DoD 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 Global Security

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

As a result of the recent establishment of the position of the ASD(Cyber Policy), I understand the Department is evaluating the future cyber policy roles of the new ASD (Cyber Policy) and PCA, as well as other leaders involved in the formulation of the Department's cyber policy, such as the USD(Policy), the ASD(Space Policy), and the DoD CIO. If confirmed, I will partner with USD(Policy) and DoD CIO to ensure alignment as these changes are implemented.

The Department of Defense Chief Information Officer

The DoD Chief Information Officer (CIO) is the PSA and advisor to the Secretary of Defense and Deputy Secretary of Defense on policy, oversight, guidance, and coordination for all Department of Defense matters related to architecture and programs related to the networking and cyber defense architecture of the Department; information resource management; information technology; electromagnetic spectrum, including coordination with other Federal and industry agencies; coordination for classified programs; and in coordination with the Under Secretary for Personnel and Readiness, 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 National Security Agency. If confirmed, I look

forward to working closely with the Chief Information Officer on matters regarding USCYBERCOM's and NSA's responsibilities.

The Chairman of the Joint Chiefs of Staff

The Chairman of the Joint Chiefs of Staff is the principal military advisor to the President, National Security Council, and Secretary of Defense. Communication between the President or the Secretary of Defense 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 or she 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 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 to provide 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 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 of Defense 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.

The Director of the Defense Information Systems Agency

The Defense Information Systems Agency (DISA) is a DoD Combat Support Agency that provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support of national leaders, joint warfighters, and other mission and coalition partners across the full spectrum of operations. The Commander, USCYBERCOM, must maintain a close relationship with the DISA Director to coordinate and represent requirements in this mission area in order to accomplish assigned missions. If confirmed, I look forward to working closely with the DISA Director on matters of shared interest and importance.

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 of Defense, 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 DoD's senior official responsible for the acceleration of adoption of data, analytics, and 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 DoD and OSD component heads, to integrate efforts to build enduring advantage for the Department and the nation.

The National Cyber Director

The National Cyber Director is the principal advisor to the President on cybersecurity policy and strategy, and leads whole-of-government coordination of programs and policies to improve the cybersecurity posture of the United States, increase information and communications technology

security, understand and deter malicious cyber activity, and advance diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace, among other matters. If confirmed, I look forward to working with the Office of the National Cyber Director in coordination with DoD officials to integrate USCYBERCOM efforts with the rest of government to deter and disrupt cyber threat actors and build enduring advantage for the nation in cyberspace.

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 my predecessors have each enjoyed with the CISA Director to deter, prevent and disrupt threats to the nation's information systems and critical infrastructure.

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 principal threats to national security stem from the People's Republic of China, which continues to challenge the United States on a global scale while seeking to expand its malign influence, and Russia, which remains engaged in unlawful military aggression in Ukraine and malicious cyber activity. We must constantly posture to gain and maintain enduring advantages throughout the competition/crisis/conflict continuum. Our ability to move with agility and seize fleeting opportunities in our campaigning efforts rest on rapid maturation of USCYBERCOM's service like authorities to: improve readiness across the force; implement new technologies; and scale capabilities that will outpace the threat.

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?

In my view, the principal threats to national security stem from the People's Republic of China, which continues to challenge the United States on a global scale while seeking to expand its malign influence, and Russia, which remains engaged in unlawful military aggression in Ukraine and malicious cyber activity. We must continue to execute our mission to deliver outcomes against National priorities in foreign intelligence, cybersecurity, protecting our national security systems and provide combat support to the Department of Defense. To do that, we must focus on strengthening the workforce, ensuring a culture of compliance, investing to leverage new technologies, and focusing on threats facing the Nation, especially the pacing challenge posed by the People's Republic of China.

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

If confirmed, I will perform a review of both USCYBERCOM and NSA's plans and approaches to our missions and emerging requirements; gain better understanding of challenges, gaps, and opportunities; and then work with Congress, the Department, and the DNI to address requirements and adjust approaches in each area as required.

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

If confirmed as the Commander of USCYBERCOM, my priority lines of efforts will be People, Innovation, and Partnerships. People are the foundation of everything we do; therefore, we must carefully mature the entire talent management lifecycle in order to improve training and readiness. We must stay on the cutting edge of new innovations and technological advances, especially in terms of artificial intelligence and advanced computing, to build and maintain warfighting advantage. And finally, we will expand capacity by ensuring trusted collaborative relationships with our combatant command, interagency, international partners, and academia and industry.

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

If confirmed as the Director of the NSA/Chief of the CSS, I will use the same priority framework described above: People, Innovation, and Partnerships. I will focus on ensuring the health and effectiveness of NSA's world-class personnel in delivering outcomes against National priorities and providing combat support to the Department of Defense. I will look for opportunities to invest in new technologies that will allow us to outpace threats facing the Nation-especially the pacing challenge posed by the People's Republic of China. And finally, NSA's ability to work in collaboration across the interagency, the private sector, and foreign partners is one of the agency's greatest strengths and critically important to our nation's success in a world of accelerating change.

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?

In my current role, I have seen first-hand USCYBERCOM's positive interactions with the Senate Armed Services Committee (SASC) and Congress. Our relationship is strong, built on transparency and responsiveness, and supports the requirements of advancing USCYBERCOM's mission and ensuring oversight. Members of the SASC have been very supportive of USCYBERCOM through office calls, briefings, hearings and visits. Additionally, SASC professional staff members (PSMs) have supported USCYBERCOM through meetings, attendance at conferences and staff delegations. These efforts help build relationships and ensure

a common understanding to include capabilities, threats, authorities and mission execution. If confirmed, I look forward to maintaining and growing this relationship.

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 law. I will build upon the close relationship 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?

In my view, the principal threats to national security stem from the People's Republic of China, which continues to challenge the United States on a global scale while seeking to expand its malign influence, and Russia, which remains engaged in unlawful military aggression in Ukraine and malicious cyber activity. However, threats to our Nation's security are numerous – actors such as Iran and North Korea attempt to coerce their respective regions with both conventional and cyber weapons, while terror groups, malicious cyber actors, and drug cartels present ongoing and transnational threats. Rapid changes in the technological environment will require the constant development of new and better approaches in response to these threats to maintain the safety of the Nation and our allies. USCYBERCOM is addressing these challenges through a constructive plan that secures, operates and hardens our critical networks in addition to reinforcing the fabrics of our international partners.

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

We face a challenging and volatile threat environment, and cyber threats to our national security interests and critical infrastructure rank at the top of the list. Rapid changes in the technological environment will require the constant development of new and better approaches in response to these threats to maintain the safety of the Nation and our allies; this will be a priority for me if confirmed. USCYBERCOM must continue to impose costs on our adversaries whenever we detect them conducting reconnaissance, espionage, influence, and even attacks in cyberspace.

16. What are your views on Russia's cyber capabilities as well as intentions in light of the invasion of Ukraine?

Russia is a highly capable cyber adversary, possessing deep technical knowledge and advanced tools, tactics, and techniques. Its cyber actors employ these capabilities to conduct information operations, cyberespionage, and cyberattacks using open source, commercially available, and custom-developed tools to persistently target government networks, commercial networks and

critical infrastructure within the United States, EU, and NATO. Cyber espionage likely remains the most persistent cyber threat from Russian government cyber actors. Russia will likely continue to integrate cyberwarfare into its military plans and operations to keep pace with USCYBERCOM efforts, and conduct cyberspace operations in response to perceived domestic threats.

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

The People's Republic of China poses one of the most advanced cyber threats to the United States and employs its capabilities to support Beijing's political, diplomatic, and military goals. The People's Liberation Army (PLA) is investing in strong cyber capabilities as a counterbalance to U.S. military superiority by exploring options to attack essential warfighting networks and critical infrastructure supporting U.S. military operations and other U.S. Government activities. If Beijing feared a major conflict with the U.S. were imminent, the PRC might consider conducting aggressive cyberspace operations against U.S. critical infrastructure and military assets worldwide.

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 its allies. State actors conduct malicious cyber activity to collect intelligence, conduct attacks, and generate revenue to bypass sanctions and fund regime goals (to include its nuclear and missile programs). North Korea continues to adapt to global trends in cybercrime by stealing cryptocurrency to bring in significant amounts of revenue.

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 networks and data. Iran likely considers its cyber program as an important tool to retaliate and gather intelligence against adversaries, as demonstrated by Iran's cyberattack last year against Albanian government networks. Domestically, Iran uses its capabilities to help control the 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 marginal limited offensive cyber capabilities, and those they do have are largely unsophisticated and limited to website defacements. Transnational criminal organizations 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.

21. Do you believe that China and Russia are engaging in cyber cooperation activities with other U.S. adversaries to help amplify the impact and effect of their cyber operations against the United States?

The PRC is unlikely to engage in cyber cooperation with other U.S. adversaries outside of a specific subset of activities, that include: attempting to set new norms in cyberspace governance, collaborating on cybersecurity by exporting Chinese information technology hardware and software, and as demonstrated following Russia's invasion of Ukraine, the spreading of disinformation that amplified Russia's themes against the United States and NATO. Russia is unlikely to share capabilities and accesses with other U.S. adversaries, as these remain largely the purview of Moscow's intelligence agencies. Cyberspace operations collaboration among adversary intelligence agencies is low and distrust is high.

U.S. Cyber Command Missions

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

In line with Title 10, U.S. Code, 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.

23. How do you define the role of the National Cyber 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) focuses on countering cyber threat actors and maneuvering against those adversaries to preclude malicious cyberspace activities, including cyberattacks and to shape adversary behavior. CNMF accomplishes this by executing cyber operations, building and refining the processes to share adversary threat data across the government and with industry; engaging with sector-specific agency partners to help them build greater resiliency within our critical infrastructure; and supporting a whole-of-nation approach to deter malicious cyber activities.

24. Do you believe the existing command and control relationships between U.S. Cyber Command and the geographic combatant commands need to be reevaluated given the need and opportunity to provide cyber support to tactical military operations?

No, not at this time. The current command and control relationship between USCYBERCOM and the geographic combatant commands enables effective employment of cyberspace operations to achieve our assigned missions. The Department reached this model over years of

maturation, which includes a close working relationship between the Combatant Commands' leadership, a heightened emphasis on the general support relationship between the Joint Force Headquarters-Cyber (JFHQ-C) and the other combatant commands, and the direct support of the Cyberspace Operations – Integrated Planning Elements established within each combatant command staff. This model has proven itself through multiple crises and is one I intend to continue to support, if confirmed.

25. How successful has U.S. Cyber Command been at integrating its national defensive, national offensive, and command support missions with the missions and kill chains of the non-cyber operational components of the Department of Defense?

The success of USCYBERCOM's integration across the Department and its warfighting domains has been proven out through several crises. We have shown ourselves to be adaptive and responsive through the employment of the Cyber National Mission Force (CNMF) and Joint Force Headquarters-DOD Information Network (JFHQ-DODIN) for national requirements. USCYBERCOM supports requirements of other combatant commands via our general support assignment of the Joint Force Headquarters-Cyber (JFHQ-C), and the direct support of the Cyberspace Operations – Integrated Planning Elements.

26. 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 Missions Force?

Congress and the Department of Defense have given USCYBERCOM significant authorities to address the issues. Some of these authorities include Enhanced Budgetary control (EBC); establishing standards for Joint cyberspace training; strategy, doctrine and tactics development; and an expanded role in acquisition. Additionally, our Cyber Excepted Service (CES) enables us to offer civilian cyber professionals opportunities to use their skills in support of the Command. These authorities allow USCYBERCOM to align its priorities, in partnership with the Services, with its ability to execute more effectively.

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. USCYBERCOM has an important role to play in cyber-enabled information activities, but 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, and the Services.

28. Do you agree with 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.

I absolutely agree. As the co-lead of the Russia Small Group during the 2018 mid-term elections, as the USCYBERCOM lead for the NSA-USCYBERCOM Election Security Group in 2020, and, as Deputy Commander of USCYBERCOM, overseeing USCYBERCOM's support to defend the 2022 U.S. elections from foreign actors, I have seen the scale of our operations and our partnerships grow exponentially. The sustained focus on this mission by NSA and USCYBERCOM, enables speed, agility, and breadth of operations to persistently engage these adversaries and postures the organizations to defend against foreign threats to the 2024 election.

National Security Agency (NSA) Missions

29. What is your understanding of the NSA mission?

It's my understanding that NSA's principal missions, SIGINT and Cybersecurity, are key to the safety and security of our nation. The NSA's SIGINT mission plays a vital role in our national security by providing America's leaders with the critical foreign intelligence they need to defend our country, save lives, and advance U.S. goals and alliances. The cybersecurity mission prevents and eradicates threats to U.S. National Security Systems (NSS), as well as identifying cyber threats the defense industrial base (DIB) and the U.S. military's weapon systems. NSA's SIGINT and Cybersecurity missions are also critical to fulfillment of NSA's combat support responsibilities.

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

NSA is responsible for securing NSS as well as preventing and eradicating threats to NSS with a focus on the DIB and the U.S. military's weapon systems. NSA also produces cyber threat intelligence products for a wide array of consumers, including making many of these products available to the public.

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 NSA provides to other combatant commands?

The signals intelligence and cyber operating environments intersect in an inextricable way. As a foreign intelligence organization and a Combat Support Agency (CSA), NSA plays a significant role in generating timely and relevant intelligence that supports operational commands like USCYBERCOM. NSA's Signals Intelligence mission and the Agency's role in cybersecurity are complementary to USCYBERCOM's role in cyberspace operations and, thus, provide a unique opportunity for collaboration.

32. In your view, in developing capabilities to support the objectives of regional combatant commanders in a conflict, should U.S. Cyber Command explore the development of strategies and operational objectives that are separate from those of kinetic conventional forces? Or should U.S. Cyber Command continue to strive to complement and reinforce traditional forms and modes of warfare?

USCYBERCOM should strive to do both. USCYBERCOM should employ strategies and operational objectives that support the Combatant Commands both defensively and offensively in support of the Joint Force. In close coordination with the other combatant commands and the interagency, USCYBERCOM should also develop strategies to defend forward by leveraging unique authorities and capabilities to degrade nation-state cyber actors seeking to target the DoD or U.S. critical infrastructure.

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

As the President articulated in recent Executive Order (EO) 14086, which was issued on October 7, 2022, the United States collects signals intelligence so that decision makers have access to the critical information necessary to advance the national security interests of the United States and to protect its citizens and allies from harm. The signals intelligence capabilities of the United States are of the utmost importance to the ability of the Executive Branch to protect our security, but such capabilities also come with tremendous responsibilities and obligations, to include ensuring that all persons are treated with dignity and respect, despite their nationality, and that all persons have legitimate privacy interests in the handling of their personal information.

From my current perspective and information made known to me through my current position, I believe that all of NSA's signals intelligence activities are authorized and consistent with the principles recently articulated by the President in EO 14086. Among others, NSA's signals intelligence activities are authorized and undertaken in accordance with the Constitution and applicable statutes, EOs, proclamations, and other Presidential directives. Further, NSA's activities are subject to appropriate safeguards, and are only conducted in a manner that is proportionate to the validated intelligence priorities for which they have been authorized. Finally, NSA conducts all of its signals intelligence activities in pursuit of only those legitimate objectives contained within EO 14086. NSA does not conduct signals intelligence collection capabilities for any of the prohibited objectives identified in the EO. If confirmed, I would ensure that NSA's signals intelligence activities will continue to be carried out in adherence to all safeguards contained within EO 14086.

34. Do you believe that the NSA is appropriately transparent about its surveillance priorities and processes? If improvements are possible, how do you intend to ensure that they are carried out?

Transparency in the IC is a balancing act, since the IC cannot perform its mission effectively unless it protects its classified intelligence sources and methods from disclosure to the Nation's adversaries. Maintaining public trust, however, is essential for the IC to be successful in its foreign intelligence mission. If confirmed, I would ensure that NSA complies with the letter and spirit of the Constitution and statutes, and exercises candor with all overseers across all three branches of government. Additionally, NSA must make available to the public information about its activities to the greatest extent possible.

Section 702 of the Foreign Intelligence Surveillance Act

Section 702 of the Foreign Intelligence Surveillance Act will expire at the end of calendar year 2023 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.

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

As a current customer of Foreign Intelligence Surveillance Act (FISA) Section 702derived products, I recognize the value and importance of this key authority in providing unique foreign intelligence to fulfill national priorities. In my experience, intelligence derived from Section 702 has been critical in counterterrorism, cybersecurity, counterintelligence, countering international drug trafficking, and strategic competition. It is also my understanding that all of the President's intelligence priority topics reported on by NSA were supported by Section 702. I defer to the White House, ODNI, DoD, and NSA leadership, however, to fully characterize the value of this authority. If confirmed, I commit to working with Congress to ensure that surveillance conducted pursuant to Section 702, and all activities governed by FISA, are performed consistent with the Constitution, U.S. law and policy.

36. 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?

If confirmed, I will be in a better position to evaluate the specifics of NSA's Section 702 compliance and oversight systems. From my current vantage point I am aware that NSA has a robust compliance regime designed to ensure adherence to all statutory and procedural requirements, including those relating to Section 702. I know NSA's workforce is dedicated to compliance with the laws and policies that govern NSA's missions, including its Section 702 activities. NSA has a dedicated corporate compliance organization, and has instilled a culture of compliance within its workforce. Based on my prior experiences, I know that NSA's compliance team is part of each stage of the analytic process—from initial targeting decision to review of the responsive content—supporting the mission and ensuring that NSA's culture of compliance is maintained day in and day out.

Where possible, and consistent with the need to continue to protect classified sources and methods, NSA and the U.S. Intelligence Community have publicly released materials describing the compliance processes in place that pertain to Section 702. For example, NSA's Section 702 targeting, minimization, and querying procedures are all available to the public with minimal redactions. These documents describe how NSA uses Section 702 to target the communications of non-U.S. persons located outside of the United States to collect foreign intelligence, and the protections that NSA applies to ensure that NSA properly handles any U.S. person information within Section 702 collection. Additionally, NSA's Section 702 activities are overseen by an internal compliance organization as well as NSA's independent Inspector General. Every NSA Section 702 targeting decision is reviewed by the Department of Justice (DoJ), and NSA must report any incidents of non-compliance to DoJ and the Office of the Director of National Intelligence. DoJ attorneys investigate each potential incident of non-compliance, work with

agencies to remediate any such instances, and report any incidents of non-compliance to the FISC and to Congress.

37. 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 NSA's mission?

Although I am generally familiar from sources such as the IC's Annual Statistical Transparency Reporting that NSA at times performs queries relating to U.S. persons, this is an issue I have limited familiarity in my current role with USCYBERCOM. At this time, I defer to current NSA leadership to fully characterize the impact to NSA's missions and other aspects of the current efforts taking place under this authority. If confirmed, I fully commit to working with Congress on all matters related to this important authority.

38. If 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?

If confirmed, I would be in a better position to judge how technically feasible such a change would be for NSA systems, and whether that would negatively impact the ability of NSA to carry out its missions effectively.

39. 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?

Based on training and past experience, I am aware that NSA, as a component of the Department of Defense (DoD), is required to follow the Attorney General (AG)-approved procedures contained in DoD Manual 5240.01 when the Agency conducts activities pursuant to authority granted by EO 12333. NSA's signals intelligence (SIGINT) activities are further regulated by the AG-approved procedures contained in the Manual's SIGINT Annex (DoDM S-5240.01-A). In general, DoDM 5240.01 permits DoD components to evaluate U.S. person information (USPI) acquired during intelligence activities to determine if the USPI qualifies for permanent retention. The SIGINT Annex adopts all of the requirements contained in the Manual, but places additional restrictions on the circumstances under which NSA may conduct queries of raw SIGINT information to intentionally retrieve communications of or concerning a U.S. person. The SIGINT Annex permits multiple types of U.S. person queries of raw SIGINT without requiring a probable cause finding, and I understand that many of these queries can be approved internally by NSA personnel. Examples include, but are not limited to situations where the U.S. person:

1) has consented to the query;
2) appears to be a victim of foreign cyber activities;
3) is being held overseas as a hostage of a foreign power; or
4) may be referenced in a foreign power dataset.

Combat Support Agency

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

Under Title 10 of the U.S. Code, as amended by the Goldwater-Nichols Act, a Combat Support Agency (CSA) is one that provides combat support or combat service support functions to joint operating forces across a range of military operations and in support of Combatant Commanders executing these operations. CSAs perform support functions or provide supporting operational capabilities, consistent with their established directives and pertinent DoD planning guidance. The combat support mission of a CSA is that portion of its mission involving support for operating forces engage in planning for, or conducting, military operations, including support during conflict or in the conduct of other military activities related to countering threats to U.S. national security.

41. 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?

USCYBERCOM follows standard processes for submitting signals intelligence requirements to NSA to enable combat support. As cyberspace domain partners, NSA and USCYBERCOM have distinct and complementary authorities. If confirmed, I will direct clear recognition across both NSA and USCYBERCOM that each organization has separate roles, resources, and responsibilities, and that our inter-service support agreements, memoranda of understanding, and special partnership agreements 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.

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

It's my understanding that the CJCS is required by law to submit biennial assessments to Congress of the responsiveness and readiness of each CSA to support the combatant commands (CCMDs). In my current position, I do not have insight into how NSA has performed in these assessments, but if confirmed, I look forward to reviewing the CJCS's assessment of NSA.

43. What is your understanding of how the Director of National Intelligence has expressed concern, if any, that the support NSA provides to U.S. Cyber Command is excessive or unjustified in light of NSA's role as a combat support agency or as a cyberspace domain partner with Cyber Command under the dual-hat arrangement?

Last year the DNI and the Secretary of Defense commissioned a study of the dual-hat arrangement led by the former Chairman of the Joint Chiefs of Staff, Ret. General Joseph Dunford. The review found that the dual-hat arrangement provided substantial benefits for the nation. The study found that although there have been concerns in the past with respect to

structure, budget, and oversight, any negative effects in these areas have been effectively mitigated by agreements and processes now in place to ensure clear accountability, cost reimbursement, and oversight. Following a review of findings from the Joint Study, the Secretary of Defense, Director of National Intelligence, and Chairman of the Joint Chiefs of Staff agree that it is in the best interest of the Nation to maintain the Dual-Hat leadership arrangement of the National Security Agency (NSA) and the United States Cyber Command.

Act of War in Cyberspace

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

It is generally accepted that cyber operations that cause death, injury, or significant damage to property would likely be considered a use of force, triggering a nation's inherent right of self-defense under international law. Ultimately, whether an act in cyberspace warrants a U.S. response in self-defense is a determination for our civilian leadership.

45. 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. policy and domestic and international law provide a sufficient framework and decision space to advise our civilian leadership whether malicious cyber acts, alone or in concert with other acts, warrant invoking the U.S. right to use force in self-defense.

46. 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.?

As with malign activity in any other domain, Departmental leaders, in coordination with the Intelligence Community, the State Department, and other key Executive Branch partners, are able to assess and advise the President whether malicious cyber acts alone or in concert with other acts, are sufficient to invoke the U.S. right to use force in self-defense. It is important to note that malicious cyber activities that do not constitute hostile acts of aggression may nonetheless cause strategic effects, constitute violations of other international legal rules or international norms, or warrant appropriate responses.

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

47. 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?

DoD employs the military instrument of national power while defending the homeland from foreign threats abroad. DoD, through USCYBERCOM and NSA, works together with a larger

Executive branch team to defend the Nation from malicious cyber activity, including cyber attacks. In order to defend the nation from malicious cyber activities, the Department can defend forward in three ways: generating insights about the threat; providing advice to Federal, state, local, and foreign partners to enhance their defenses; and, acting when necessary and consistent with DoD's authorities, to disrupt adversary cyber actors. DoD may also provide defense support of civil authorities, upon request, should a cyber incident exceed the capacity of another department or agency.

48. 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 works abroad to persistently engage foreign malicious cyber actors who threaten U.S. critical infrastructure. Through Hunt Forward missions, where we deploy teams of cyber operators to work with allies and partners to find and enable them to defend against malicious cyber actors operating on foreign partner networks, we discover cyber threats before they reach the United States. These operations do several things: they enable USCYBERCOM to posture to take action to disrupt the threat to the United States, they strengthen partners and Allies' defenses, and they give us insight into new threats. We then share that threat information with domestic partners like the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and with industry to enable measures to harden cyber-defenses here at home.

49. 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?

When requested by another Federal department or agency and approved by the appropriate DoD official, or as directed by the President, DoD responds to a cyber incident pursuant to the long-standing Defense Support of Civil Authorities (DSCA) process. The DoD weighs each DSCA request individually to determine if it has sufficient capability and capacity to support. Through collaborative partnerships with NSA, DHS/CISA, U. S. Northern Command (USNORTHCOM) and/or U.S. Indo-Pacific Command (USINDOPACOM), the National Guard Bureau, and others, USCYBERCOM is well-postured to respond to such requests when they occur.

50. 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?

As an active component military force, USCYBERCOM's mission and authorities are focused on foreign operations against foreign actors. The command does not conduct operations inside the United States, but enables those domestic partners with appropriate authorities, including the Department of Homeland Security and the FBI. As directed, USCYBERCOM can support civil authorities to defend U.S. critical infrastructure from malicious cyber activities in and through cyberspace, in coordination with or in support of USNORTHCOM and/or USINDOPACOM in the exercise of their homeland defense and DSCA missions.

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

The National Guard is both a force multiplier for USCYBERCOM missions and a critical capacity for their states. Many of our U.S. National Guard and Reserve members have significant and relevant private-sector experience and can rapidly share appropriate information on malicious cyber activity with state and local authorities. These members can conduct state-authorized operations domestically under state law to protect critical infrastructure while in a state active-duty status or , if need be, can be mobilized on Federal active-duty to join the USCYBERCOM mission directly.

52. 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?

U.S. policy is to use all instruments of national power to counter cyber attacks and malicious cyber activity of foreign adversaries that target the United States and threaten our national security. Executive Branch policies prioritize enhanced cybersecurity for U.S. critical infrastructure and National Security Systems, and DoD has been granted statutory authorities to conduct appropriate and proportionate military activities in foreign cyberspace to disrupt and defend against foreign malicious cyber activity directed against our government, people and critical infrastructure. These policies have contributed to DoD's ability to recognize and mitigate these threats in collaboration with domestic and international partners.

Deterrence Through Cost Imposition

Multiple annual threat assessments of the U.S. Intelligence Community have concluded that the People's Republic of China (PRC) would attack U.S. critical infrastructure through cyber operations if Beijing decided to invade Taiwan and expected the United States to intervene. The Defense Science Board (DSB) Task Force report on Cyber Deterrence, issued in February 2017, concluded that it is critical for the Department of Defense (DOD) 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 Defense 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."

53. What are your views on the conclusions and recommendations of this Task Force?

I believe that USCYBERCOM's role in campaigning in cyberspace below the level of armed conflict is critical to reinforce deterrence and to impose costs on our adversaries. The DSB study predated Congress' action on declaring cyber a domain of traditional military activity, enabling

alignment of U.S. law, policy, and authorities to DoD. The 2023 National Cyber Strategy and 2023 DoD Cyber Strategy—which nests within the 2022 National Defense Strategy (NDS—address many of the areas of the DSB study by clearly and publicly articulating that all tools of national power will be used in a more intentional, more coordinated approach to cyber defense. For the Department of Defense, that means that USCYBERCOM will work with the interagency, private sector, and our partners and allies to deliver cyberspace options in combination with other kinetic and non-kinetic capabilities to deter, disrupt, and respond to malicious cyber actors.

54. Do you believe it is important to adopt and articulate a cost-imposing deterrence strategy based on credible options for responding against targets that adversaries' value with offensive cyber operations to cyber attacks against U.S. critical infrastructure?

Cost imposition is one of three DoD approaches to deterrence – all are important. DoD's potential responses, however, should not be limited to the cyber domain. USCYBERCOM is participating in Department-wide and whole-of-government collaboration and coordination efforts to reduce the perceived and actual utility of cyber attacks on critical infrastructure, and USCYBERCOM is also collaborating with Allies and partners to develop options to impose collective costs, leveraging the convergent power that remains a U.S. competitive advantage. As we implement the department's National Defense Strategy, our focus on integrated deterrence, campaigning, and building enduring advantage will support deterrence efforts to prevent strategic attacks, aggression, and defense of the homeland.

55. In light of the conclusions of the Intelligence Community, what is your assessment that the PRC is currently deterred from conducting cyber attacks against U.S. critical infrastructure?

I assess that the PRC understands the potential for a high cost in response to a cyber attack against U.S. critical infrastructure during peacetime. However, during conflict, it remains a potential option for the PRC.

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

The command supports the whole of government approach to deterrence in support of national security objectives. We implement our part on national strategic deterrence through the department's integrated deterrence effort and our role in providing cyberspace operations options to senior leadership. We can further enable this effort by investing in the resilience of the Department's Information Networks, enabling the defense of non-Department networks, building the cyber capacity of, and generating cyberspace options for, Allies and partners, and investing in strategic cyberspace attack capabilities. We will also aggressively utilize our new enhanced budget and acquisition authorities to meet future deterrence needs with the continued support, sustainment, and growth of the CMF.

<u>Dual Hat</u>

Last year, the Director of National Intelligence and the Secretary of Defense conducted a study of whether to continue the "dual hat" arrangement whereby the Commander of U.S. Cyber Command also serves as the Director of the National Security Agency.

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

Yes, maintaining the dual hat arrangement enhances the effectiveness of both organizations and is in the best interests of the nation. The signals intelligence and cyber operating environments substantially overlap. Eliminating the dual hat would reduce relevant visibility and understanding across both mission sets, increasing risk to intelligence sources and operational activities. It would reduce the speed and effectiveness of cybersecurity collaboration in the protection of National Security Systems (NSS), the DODIN, and the DIB by slowing and complicating information sharing and work with overlapping partners. Finally, ending the dual hat would complicate relationships with Allies and partners that conduct their own signals intelligence and cyberspace operations.

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

No, the demands of each position are effectively managed given the separate and distinct missions, authorities, and organizational structures senior leadership teams, staffs, and organizational structures of each organization.

59. 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?

Yes. It would be more time consuming, more complex and less effective. Fracturing the current USCYBERCOM -NSA command arrangement would degrade flexibility, adaptability, and speed of action now provided through close and interconnected processes; ultimately impacting mission outcomes.

60. 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?

All resources must be used for the purposes appropriated. NSA's budget and personnel do not subsidize USCYBERCOM. The Senior Steering Group that was commissioned to study the dual hat found that, although there have been perceptions in the past with respect to structure, budget, and oversight, any negative effects in these areas have been mitigated by agreements and processes now in place to ensure clear accountability, cost reimbursement, and oversight. If confirmed, one of my priorities would be to ensure that the teams at USCYBERCOM and NSA continue those best practices, and if necessary, build upon the activities that have made those agreements and processes effective.

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

As a result of the overlap of the signals intelligence and cyber operations environments, NSA and USCYBERCOM have developed a close partnership in this area. Under the current leadership arrangement, a single, fully informed decision maker, responsible for the separate and distinct mission outcomes of both organizations, is able to protect our nation's most sensitive signals intelligence equities while operating in defense of national interests and ensuring both organizations are aligned with the nation's priorities. If confirmed, I will continue to utilize and improve processes for identifying and evaluating the sharing of accesses, where appropriate, from NSA to USCYBERCOM, from USCYBERCOM to NSA, and with other key partners, to deliver the best outcomes for the nation.

62. 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?

This is perhaps the most critical advantage of the dual hat – a single decision maker, responsible and accountable for the mission outcomes of both organizations, is best equipped to protect critical intelligence equities while executing national priorities, as directed. It ensures fully informed tradeoff decisions are made under accountability to both the Secretary of Defense and Director of National Intelligence.

63. 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?

No. The Senior Steering Group that was commissioned to study the dual hat found that, although there have been perceptions in the past with respect to structure, budget, and oversight, any negative effects in these areas have been mitigated by agreements and processes now in place to ensure clear accountability, cost reimbursement, and oversight.

Crypto Modernization

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

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

It is my understanding that there are two overarching challenges associated with cryptographic modernization across the Department. The first is that a significant portion of the existing cryptographic inventory is, by NSA's assessment, either obsolete or approaching obsolescence –

meaning that it is within reach of today's technology and vulnerable to compromise by a sufficiently well-resourced and technologically advanced adversary.

The second cryptographic modernization challenge, more vast in scope and scale, is proactively preparing for potential future realization of a sufficiently large quantum computer in adversary hands that could break public-key cryptosystems used within the U.S. and around the world.

Modernization efforts are focused on the elimination of the already vulnerable cryptography in use today and also ensuring that the DoD's cryptographic inventory is completely quantum resistant by the year 2034.

65. 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.

In light of the threat posed by technologically advanced near peer nation states, significant changes to the oversight of crypto modernization have occurred. DoD, under Joint Staff oversight, has made tremendous strides in completing and advancing cryptographic modernization across a number of systems. However, challenges remain with completing modernization on several operational systems due to their sheer volume of material and scale of operations. Military Department sponsors of systems that are not yet fully modernized from obsolete cryptography are required to provide plans, with resources aligned, to the Joint Staff outlining their path to full modernization. Joint Staff, with NSA support, then adjudicates the way forward.

Significant planning measures are underway in DoD and, via NSM-10, have also now begun for the Federal Government at large with the goal of full modernization across Government systems by 2035 (2034 for DoD). Though this end goal is 12 years away, success in the coming years will require continued, significant inter-agency coordination as well as alignment of budgetary and technical resources needed to accomplish the goal. The DoD CIO is coordinating an integrated DoD cryptographic modernization roadmap that will be delivered to OMB this summer.

Additionally, cryptographic modernization progress across DoD is reported quarterly to the DEPSECDEF.

66. In your view, will the tracking and reporting requirements established in section 1512 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117-263) significantly improve compliance with cryptographic modernization requirements? If not, what changes to those requirements might be needed to make it more effective?

There is certainly an expectation that Section 1512 of NDAA 2023 will be effective in driving compliance and reporting of cryptographic modernization progress, reinforcing and complementing directives already in place.

67. 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?

An end goal of full post- quantum cryptographic modernization will touch the vast majority of today's cryptographic inventory, including commercial cryptographic technologies. In DoD and across the Executive Branch, this will affect almost every National Security System. NSM-10 establishes a goal of full post quantum cryptographic modernization by 2035 for the Federal Government. We believe this is a challenging, yet manageable, end goal, after which the risk accelerates in terms of the potential for adversary availability of a sufficiently large quantum computer. Within DoD, we have an excellent start and are working toward full modernization by 2034. NSA and the Military Departments issue cryptographic modernization roadmaps annually. DoD CIO, NSA, and the Military Departments are collaborating on delivering an integrated DoD cryptographic modernization roadmap and implementation plan later this Summer. At the Federal Government and commercial level, the National Institute of Standards and Technology (NIST) is aggressively leading the assessment and selection of commercially available quantum resistant cryptographic algorithms and protocols.

Radio-Frequency Enabled Cyber Operations

It is recognized that a wide variety of military systems may be vulnerable to cyber attacks through radio-frequency apertures. These systems include command and control networks, data links, sensor systems (both active and passive), weapons platforms and systems, and navigation systems. Section 1647 of the National Defense Authorization Act for Fiscal Year 2016 required the Department of Defense (DOD) to assess and remediate the cyber vulnerabilities of all major weapons systems. However, these assessments reportedly did not factor in the attack vector presented by radio-frequency apertures.

68. In your view, do you think that the Department of Defense is sufficiently focused on the threat posed by Radio-Frequency (RF) enabled cyber attacks?

The Department needs to be able to identify, characterize, and generate agile responses to all shapes and forms of threats, that include RF threats, based on intelligence driven assessments as well as assessments of individual weapons systems. RF-enabled cyber threats pose real risks to operation of weapons systems, but must be considered in context of a full risk analysis and addressed as part of system-wide mitigations.

69. Do you think such threats should be addressed by such vulnerability assessment programs, such as the one mandated by section 1559 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117-263)?

While the assessment programs defined in section 1559 of the NDAA are a good start, the implementation and robustness of those assessment programs are key to accurate assessment of warfighter mission risk, and to applying full-spectrum mitigations. The most important value of

the programs defined in section 1559 will be informing overall cyber risk assessments of weapons systems and expanding the scope of potential mitigations against cyber threats.

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

Expeditionary cyber forces have already demonstrated potential to extend the reach of cyber enabling activities and close the gaps that limit cyber forces' ability to access important tactical targets in forward locations. If confirmed, I will work with the Services to ensure any tactical forces will meet USCYBERCOM training standards, follow Department deconfliction policies, and when leveraging USCYBERCOM authorities, ensure interoperability with Joint Cyber Warfighting Architecture.

71. 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.

If confirmed, I will work closely with the Services and geographic combatant commands as we study the issue to include training, standards, interoperability, and authorities to implement requirements under Section 1510 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, *Integrated Non-Kinetic Force Development,* to optimize the delivery of effects.

72. 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 the operational concepts needed to enable such operations at an adequate pace?

Yes. The nature of modern network-centric warfighting is such that nearly every piece of electronic equipment represents a potential cyber-attack surface, to include tactical military systems. USCYBERCOM capabilities are always evolving to take advantage of cutting-edge technology, research, and development. Just as we continually improve our own defenses against novel cyber threats, so do our adversaries; if confirmed, it is my intent for the Command to seek new and innovative means, methods, and doctrine to achieve our mission and provide a comprehensive suite of non-kinetic effects when called upon to do so.

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

Yes. In my opinion, developing new and novel capabilities and approaches to deliver non-kinetic effects will benefit the Combatant Commands and the Services. The unique value of the cyber domain is that it crosses, supports, and enhances every warfighting domain by ensuring the secure operation of the Department's decision-making systems, disrupting malicious cyber actors' capabilities and ecosystems before they can threaten our networks and platforms, and, when called upon, deliver non-kinetic effects to enable Joint Force Commanders to achieve early initiative during contingencies.

Enhanced Budget Control (EBC)

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.

74. In your view, what impact, if any, has the EBC authority had on the resources allocated to the cyber mission?

EBC authority allows USCYBERCOM to articulate cyber resource requirements directly into Department PPBE processes. EBC authority will allow USCYBERCOM to ensure resources for Cyber Mission Forces (CMF) are aligned with the USCYBERCOM Commander's priorities. These resources fund the CMF Teams, their operational headquarters, the Cyber National Mission Force Headquarters, the USCYBERCOM Headquarters, the cyber planning elements at each Combatant Command, and the development and fielding of the capabilities required by each of those organizations needed to conduct operations.

75. In your view, is the increase in funding in the President's Budget Request for Fiscal Year 2024 a result of actions taken due to EBC invested in the Command?

The President's Budget Request for Fiscal Year (FY) 2024 includes increased funding for readiness, forces, and capabilities. Select programs with requested funding increases include: the Persistent Cyber Training Environment, continued growth of the Cyber Mission Force, and the Joint Common Access Platform.

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

This transition is ongoing. We effectively participated in the Department's process to build the President's Budget for FY 2024. Funding the FY 2024 budget request will allow USCYBERCOM to demonstrate competence in execution of EBC. Concerns remain about the impact of a FY 2024 continuing resolution. A continuing resolution will delay the implementation of EBC and generate a significant amount of re-work based on the shift in appropriation between FY 2023and FY 2024.

77. 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?

USCYBERCOM has not seen any indications that the military services will reduce their level of support for the Cyber Mission Forces. We will continue to partner with the services in a number of areas, to include: the assignment and initial training of their military personnel, some administrative and logistics support for their teams, as well as basic research and intelligence analysis.

78. What mechanisms do you have to monitor and respond if the services take such action?

There are a number of mechanisms that will allow USCYBERCOM to monitor and respond if the services reduce their level of support. We will have an opportunity to review each service's program and highlight any issues during DoD's program budget review process. We will also be able to engage with the Principal Cyber Advisor and the Chief Information Officer to monitor and respond to unanticipated reductions in the levels of support from the services.

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. However, there has been some support for creating a separate Cyber Force, partly in response to persistent readiness problems.

79. 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.

We have patterned USCYBERCOM after the U.S. Special Operations Command (USSOCOM) model that vests Service-like authority within a combatant command. USSOCOM has proven that this model is successful in leading a formidable capability for our nation. Congress and the Department have set the conditions for U.S. Cyber Command to achieve this same success, leveraging expanded acquisition authorities and enhanced budget control to train and equip our cyberspace forces. These tools are just now coming to a point that will allow the command to ensure prioritization, resource allocation, and efforts to deliver the necessary cyber systems and capabilities. We should continue this approach to allow adequate time to see the results of these authorities in improving the readiness and capabilities of our cyberspace forces. Additionally, there are several statutorily-required tasks from the FY 2023 NDAA that are currently underway to examine readiness and force generation challenges. If confirmed, I will work with Congress to understand the results of these assessments and any associated recommendations for improving the USSOCOM-like model for U.S. Cyber Command.

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

The success of our operations to support the 2022 National Defense Strategy depends on training and readiness. We have prioritized improving the readiness of our cyber forces since USCYBERCOM became a unified Combatant Command in 2018, and there has been progress. With the passage of the FY 2024 budget, USCYBERCOM will now have the USSOCOM-like authorities and resources to improve readiness and capabilities across the force. Changing course to stand up a new Cyber Service before allowing sufficient time for these authorities to impact readiness would be premature, necessitating significant additional resources and would actually detract from our efforts to improve readiness over the next 3-5 years.

81. 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.

For USCYBERCOM, FY 2024 is the first year USCYBERCOM will be able to fully realize the opportunities provided with the newly granted EBC and service-like authorities. The command will work with the Services to develop a strategy to increase and sustain readiness by prioritizing billets for CMF that require sustained, high fill rates from each service; codifying assignment policies that ensure at least two consecutive tours in the CMF; improving service-level training courses; providing consistent incentives across the services to recruit and retain the best cyber talent; and standardizing cyber readiness reporting requirements. If confirmed, I will brief Congress on the progress of these efforts and any further recommendations.

82. 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, I do not think it is necessary to enhance the authority of the Commander of USCYBERCOM in the area of personnel policy, training, and retention in order to ensure stability in the readiness of the Cyber Mission Force. Our service-like authorities allow the Commander to establish readiness standards for the Department and at the same time identify unique service initiatives that could be scaled into Departmental policy/practice.

Impact of Artificial Intelligence/Machine Learning

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. Subject to appropriate human controls, in the cyber domain, AI may enable even modest numbers of cyber operators to achieve much greater levels of scale, speed and impact. However, in contrast, intelligence collection operations in cyberspace are generally characterized as slow, methodical, and manually intensive because of the care that must be taken to avoid detection. U.S. Cyber Command, having emerged from the U.S. signals intelligence (SIGINT) culture, remains strongly influenced by the SIGINT community's tactics, techniques, and procedures and emphasis on careful preparation and covert tradecraft.

83. Is there potentially a different model for operating in cyberspace that would be more conducive to the application of AI to achieve scale and speed in offensive cyber operations? For instance, could focusing on exploiting known vulnerabilities with existing, well-known tools make it easier for AI technologies to be adapted to helping orchestrate cyber intelligence and attack operations at greater rates and scales?

AI offers a wide range of new opportunities for operating in cyberspace. When applied to the cyberspace missions, AI has the potential to enhance exploitation of vulnerabilities, improve vulnerability research and access development, and accelerate the speed and scale of many aspects of conducting cyberspace operations. USCYBERCOM is in collaboration with partners

across the Department to create the AI Roadmap and Implementation Plan for the Cyber Operations Force to determine how to most effectively utilize these new applications. As we begin executing enhanced budget control and acquisition authorities, CYBERCOM will be well postured to align and accelerate the delivery of AI capabilities to the warfighter.

84. Alternatively, are recent advances in AI better suited to supporting defensive cyber missions, where spotting and correlating anomalous but ambiguous events in noisy environments is at a premium?

AI will be a force multiplier for network defenders in threat hunting, incident response, terrain introspection, security compliance, patching, and the deployment of zero-trust policy engines. We have collaborated with NSA and our Service Cyber Components to leverage Commercial off the Shelf AI capabilities for malware analysis. USCYBERCOM continues to evaluate additional applications of AI in support of defensive cyberspace operations through the development of the AI Roadmap and Implementation Plan.

85. 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?

The enhancement of cyberspace operations with AI could be a disruptive technology change. Cyberspace operations enhanced by AI have the potential to achieve an accuracy and precision which were previously only attainable through skillful interaction between computer systems and human operators exercising strategic decision making—at a competitively advantageous scale, speed, and rate of discovery. Sustaining a global advantage will require continual adoption and evolution of both the technology and the processes, doctrine, and culture of our organization.

86. Are U.S. Cyber Command and the military services, and the defense agencies such as the Defense Advanced Research Projects Agency (DARPA), investing aggressively in AI technology in direct support to the cyber mission, and is there now a heightened awareness and acceptance of the significance of this technology for offensive and defensive cyber warfare, and information warfare more broadly?

USCYBERCOM is working to identify applications for an increased adoption of AI/ML technologies for the cyber mission. We are most mature in leveraging AI/ML techniques that are integrated in commercial off-the-shelf tools or services. Through the recently established Constellation pilot program, CYBERCOM will be able to more quickly leverage DARPA's investments in this area to mature and transition new cyber capabilities to the operational warfighter. USCYBERCOM is in collaboration to create the AI Roadmap and Implementation Plan for the Cyber Operations Force with DOD Chief Information Office (CIO), Chief Digital and Artificial Intelligence Office (CDAO), DARPA, NSA, OUSD(R&E), and other partners. We expect this to be transformative for our operations.

87. In all of these cases, what data sources or repositories are needed to enable these activities? Is the problem one of better leveraging sources we already have, or developing all new data sources and repositories?

Computational infrastructure and data sources to meet current operational requirements with AI/ML analytics largely exist across USCYBERCOM and NSA systems. The Joint Cyber Warfighting Architecture (JCWA) programs are continually working to optimize data movement and system access to expand the use of AI/ML. Establishment of the JCWA Program Office will help facilitate efforts to optimize and better leverage our current architecture.

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

China and Russia are both pursuing AI to support military decision-making, weapons systems, and autonomous vehicles. Over the past decade, China has established a robust framework to bolster its AI and made contributions to the field on a global scale. Rapid changes in the technological environment will require the constant development of new and better approaches to collection, analysis, and dissemination of intelligence about these threats to maintain the safety of the Nation and our allies; this will be a priority for me if confirmed.

Cyber Posture Review

The Department of Defense (DOD) conducted a cyber posture review, including a gap analysis, in 2022 to inform the development of the DOD Cyber Strategy and future capability planning and funding.

89. In your view, what are the most significant findings of the posture review?

In my opinion, the most significant findings of the posture review relate to people, partners and capabilities. Beginning with people, USCYBERCOM must recruit and retain the talent to efficiently and effectively perform the mission. USCYBERCOM must better integrate partners across foreign military, intelligence, and the private sector to meet growing defensive requirements by burden sharing. Finally, USCYBERCOM must invest in developing capabilities to enhance flexibility and options for cyberspace operations.

90. If confirmed, where in your priority list does addressing the gaps identified in the posture review fall?

If confirmed, my priorities are people, innovation, and partners. We have to work with the Services to bring in capable people, train them, and provide them career opportunities to retain them. USYCBERCOM must invest in the technology, capabilities, and infrastructure necessary to support the joint force. Critical to the Department's success is the ability to build and maintain strong collaboration with the agency partners, industry, academia, and our Allies and Partners to counter the threats to our national security.

91. Do you have any concerns with any significant findings and recommendations of the posture review?

The CPR highlights the use of our Cyber Protection Teams. USCYBERCOM's Cyber Protection Team is a capability that defends friendly networks, bolster tactics, technics, and produces, and enhance collaboration with Allies and partners. This supports each of USCYBERCOM's enduring missions in cyberspace and mitigates attacks against the Department's networks, the nation, and our Allies and partners. We reviewed the CPR and have incorporated feedback to improve Cyber Protection Teams operations.

National Cyber Strategy

Adversary Cyber Presence in the United States

The intelligence and military cyber forces of adversary nations such as Russia, China, Iran, and North Korea are effectively deployed and constantly operating inside the United States. However, the vast U.S. private and commercial cyberspace is largely a sanctuary for adversary cyber actors, allowing them to essentially deploy forces inside the United States and operate clandestinely. The March 2023 National Cybersecurity Strategy contends that the very technically proficient American commercial internet industry, with incentives and assistance, could provide a potent solution to this problem without impinging on privacy.

92. What is your assessment of the potential for the major U.S. Internet service providers and platforms, if incentivized and motivated, to prevent malicious cyber actors from abusing their platforms and services?

U.S. Internet Service Providers (ISPs) and platforms have an enormous responsibility and are faced with many challenges, to include the misuse and abuse of their infrastructure by foreign malicious cyber actors. Many ISPs already taken action to prevent and eradicate malicious cyber actors on their services, though more can be done. There are efforts being considered across the U.S. Government to review and implement incentives for the private sector to increase their level of cybersecurity for their products and services. NSA certainly plays a role in this effort by sharing information an ISP will need to identify foreign malicious activity in an effective and efficient manner and to educate the ISP cybersecurity personnel regarding what measures will be effective at mitigating the threats, thus reducing the resources required on the part of the company to better secure their platforms against misuse and abuse. If confirmed, I will partner with other federal agencies and continue to work with service providers on this issue.

93. How do you think the next iteration of the Cybersecurity Maturity Model Certification (CMMC) program that is in development may help improve the cybersecurity posture of businesses to defend against such malicious actors?

The theft of intellectual property from U.S. companies for both espionage and economic gains has long been a problem, especially within the Defense Industrial Base (DIB). These companies are critical to the defense of our Nation and the effectiveness of our warfighters. Therefore, it is imperative that we protect the sensitive information, operational capabilities, and product integrity created, housed, and used by the DIB to ensure the generation, reliability, and preservation of U.S. warfighting capabilities, and CMMC is a key tenet in this strategy. CMMC

will ensure baseline security is in place for organizations supporting sensitive, but unclassified DoD programs, ensuring that a minimum standard be met prior to contract award. While advanced nation-state actors will continue to pursue ways into these networks and systems, CMMC could greatly diminish both the attack surface across the DIB, and the amount of time malicious cyber actors may spend in these networks before they are detected and eradicated, ultimately reducing data theft.

94. In your view, how useful is the NSA Cybersecurity Collaboration Center in scaling this model by providing intelligence- and technology-driven cybersecurity assistance through open, collaborative partnerships with industry and the Department of Homeland Security?

From my vantage point, I believe that NSA's Cybersecurity Collaboration Center (CCC) has made tremendous strides in scaling the public-private partnership model for collective cyber defense. The U.S. technology and cybersecurity sectors build, maintain, and defend the infrastructure upon which DoD, USG, and critical infrastructure operate. We find that many of these companies are motivated to keep those technologies secure from state- sponsored malicious actors. The CCC provides information and context that helps inform and prioritize those efforts. Those companies also have unique insights through their routine business and are able to share those back with NSA to help inform its cybersecurity and foreign intelligence missions, creating an iterative communications cycle that improves the collective understanding of the actor, their activities, and ways to defend against them.

U.S. Cyber Command Role in Disruption Campaigns

The National Cybersecurity Strategy (March 2023) establishes the goal to "make malicious actors incapable of mounting sustained cyber-enabled campaigns that could threaten the national security or public safety of the United States" by disrupting and dismantling such actors.

95. In your view, would you expect that U.S. Cyber Command will be called upon to execute "sustained" offensive operations against cyber adversaries to disrupt their ability to conduct malicious operations, including operations to disrupt malicious activity before it effects its intended targets?

Yes, USCYBERCOM remains committed and ready to defend the homeland, support the Joint Force, and safeguard and advance U.S. national interests in and through the cyber domain. This requires USCYBERCOM to execute sustained cyber operations in campaigning with the combatant commands, the interagency, industry, and our Allies and partners.

Cyber Intelligence Center

Every operational domain other than cyberspace – land, sea, air, and space – has a dedicated Science and Technology and Foundational Intelligence Center. U.S. Cyber Command has concluded that the cyberspace operational domain also merits such an intelligence center.

96. What is your understanding of the result of the recent study on this topic by the Defense Intelligence Agency?

The offices of Undersecretaries of Defense for Intelligence and Security and Policy are engaged with DIA and USCYBERCOM for a review of the Command's requirement for foundational intelligence consistent with the support that every other Combatant Command receives from the Defense Intelligence Enterprise. Foundational intelligence in the domain of cyberspace is critical to conducting all of USCYBERCOM missions, and if confirmed, ensuring that Cyber Command's requirements are met will be a focus of mine.

97. In your view, is such a center is necessary?

Yes. A consolidated Cyber Intelligence Science and Technology Center would close gaps in intelligence support to cyberspace operations. If confirmed, I will work with USD(I&S) and DIA to evaluate feasibility and executability of solutions to close these intelligence gaps.

98. Do you think that NSA could provide much-needed technical intelligence if additional resources were available?

Yes. NSA's technical intelligence capabilities are superb. If confirmed, I will work with USD(I&S) to evaluate any additional resource requirements.

99. In your view, would there still be a shortfall in the provision of all-source intelligence analysis?

Yes. The Intelligence Community is still maturing all-source analysis, particularly as it relates to Order of Battle of Cyberspace Forces and targeting in the cyberspace domain.

<u>The Nature of Offensive Cyber Operations in a Conflict</u>

The NSA, as an intelligence agency, appropriately places the highest importance on remaining undetected, and accordingly invests in high-end—and therefore expensive and hard-to-develop—technical tools and tradecraft, following a deliberate methodology for developing and maintaining capability. U.S. Cyber Command, as a military combatant command, could in many circumstances have different interests and objectives. For example, it could seek the capability to act rapidly against targets for which there has been no time available to methodically access, and it may need tools and processes that can be used without fear of compromise during military operations. It could be argued that supported combatant commanders cannot wait weeks or months once a conflict has started for U.S. Cyber Command to be able to conduct follow-on operations to those which may have been pre-planned.

100. What are your views on these tradeoffs? Do you have any ideas for how to balance the competing institutional needs and goals for U.S. Cyber Command and NSA in this respect?

The most positive aspect of the dual hat is the ability of a single decision maker, responsible for the separate and distinct mission outcomes of both organizations, to allocate resources, set priorities, and execute complementary actions to produce critical outcomes for the nation. It ensures that a single, fully informed decision maker is able to protect our nation's most sensitive signals intelligence equities and ensure both organizations are aligned with the nation's priorities.

101. In your view, are there ways in which U.S. Cyber Command can operate effectively against meaningful targets in a conflict for which there has been no prior preparation?

Developing cyber capabilities in support of the Combatant Commanders in conflict is a key element of USCYBERCOM's mission. If confirmed, I welcome the opportunity to have a deeper discussion in the appropriate setting.

102. In your view, should it be accepted that the most important offensive cyber contributions to combatant commanders' objectives in a conflict will be limited to a series of unique, pre-planned operations?

Developing cyber capabilities in support of the Combatant Commanders in conflict is a key element of USCYBERCOM's mission. If confirmed, I welcome the opportunity to have a deeper discussion in the appropriate setting.

Acquisition of Accesses and Exploits and the Joint Cyber Warfighting Architecture

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).

103. 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?

Yes, JCWA's success is predicated on support from all branches of the military. In conjunction with other stakeholders, USCYBERCOM is working to establish the Program Executive Office (PEO) JCWA, as directed in FY23 NDAA Sec. 1509.

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

The military services have agreed to the establishment timeline, which will result in a PEO JCWA being fully operational by FY27. Accordingly, the Army remains responsible for sustaining the Persistent Cyber Training Environment (PCTE) and Joint Common Access Platform (JCAP). The Air Force remains responsible for sustaining Unified Platform (UP) and Joint Cyber Command and Control (JCC2).

105. In your view, is it critical that U.S. Cyber Command also receive support from the Secretary of Defense and Principal Staff Assistants to acquire the necessary acquisition expertise to manage the complex JCWA acquisition and integration challenges?

Yes. USCYBERCOM has received strong support from OSD(A&S) on this issue.

106. If confirmed, are you confident that you will receive that support? What tools or processes will you have to monitor and enforce any support commitments that need to be sustained from the services?

Yes. USCYBERCOM will use enhanced budget control and different acquisition authorities to ensure continued support from the services. Beginning in FY 2024, USCYBERCOM will meet with the service's program management offices (PMO) monthly to track fund execution status. In relation to acquisition, USCYBERCOM meets with the services PMOs quarterly to provide prioritized operational and engineering requirements for development. These regular engagements allow issues to be quickly identified and remedied.

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.

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

The Constellation program aims to quickly transition technologies, capabilities, and prototype systems into JCWA to enable full spectrum cyberspace operations to deter, disrupt, and defeat adversary cyber actors, through close coordination between the cyber mission force (CMF), DARPA and the DOD S&T community. Through streamlined acquisition, assessment, approval, deployment processes, and modern DevSecOps development processes, Constellation will enable the rapid and continuous delivery of cyberspace technologies, capabilities, and prototype systems to the warfighter.

108. 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 has substantial authorities to acquire tools and capabilities from the private sector. I will continue to work with R&E on the evolving role of USCYBERCOM in the DOD S&T community to ensure USCYBERCOM is properly postured to provide the COF with the most advanced and extensive cyber capabilities.

109. 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?

USCYBERCOM has worked to establish and maintain its private-sector relationships, which are critical to our ability to rapidly acquire cyber capabilities. Through this continued utilization of our authorities, USCYBERCOM is able to leverage internal activities, as well as partner with other Department entities, in order to acquire cyber capabilities on a scale and tempo that supports our operations.

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

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

Determinations regarding how positions must be filled are made using the guidelines in Department of Defense Instruction (DoDI) 1100.22, Policy and Procedures for Determining Workforce Mix. Planners review mission requirements and organizational structure to determine the appropriate workforce mix. The guidelines in DoDI 1100.22 identify which functions are inherently governmental, then determine which will be performed by DoD civilian employees, and which will or must be performed by military personnel.

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

Contractor-provided services support a variety of important functions for USCYBERCOM. These functions encompass vital support to both the Command, and the CMF. DoD policy requires that military operations involving the planned use of destructive capabilities, including offensive cyber capabilities, must be performed by Federal military personnel, rather than civilian or contractor personnel. Civilian and contractor personnel may perform other cyberspace operations, including support to offensive cyber operations not meeting the policy requirement described above, although contractor personnel may not perform inherently governmental functions. It is essential that Federal military personnel and U.S. government civilian employees maintain proper oversight and ensure inherently government functions are performed by government personnel.

112. 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?

As USCYBERCOM engages in worldwide operations, the mission will determine the necessary mix of active forces, the Reserve Component, DoD Civilians, and contracted workforce to achieve our military objectives. We will continue our efforts to recruit well-trained and educated professionals.

USCYBERCOM continues to achieve the appropriate force mix. USCYBERCOM has received additional civilian employee allocations under the Joint Chiefs of Staff Joint Manpower Validation Board, and these will take the command staff to a mix of approximately 41 percent

military members and 59 percent civilian personnel. This mix is appropriate given the specific functions of staff personnel.

113. 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?

Future talent management, with a focus on recruitment, retention, and equipping warfighters in targeted areas, is part of the effort to retain a high-quality workforce. We are working with the Services and across the Command to identify recruiting practices to gain talent, which is innovation and enduring advantage. We need motivated and talented people to serve our nation, and USCYBERCOM continues its commitment to attract candidates with a wide range of backgrounds and experiences.

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.