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

Defense of Defense Reforms

The National Defense Authorization Acts for Fiscal Years 2016 and 2017 enacted sweeping reforms of the organization of the Department of Defense—both military and civilian, including the elements created by the Goldwater-Nichols Department of Defense Reorganization Act of 1986—in order to enhance the effectiveness of the Department of Defense in the execution of the National Defense Strategy in the 21st Century. These reforms directed the elevation of U.S. Cyber Command to a Unified Combatant Command, restructured the Office of the Secretary of Defense, particularly with respect to the Under Secretary of Defense for Acquisition, Technology, and Logistics, returned more authority to the military services for program management, and created additional acquisition pathways.

Based on your experiences as a senior officer, what challenges have you observed with the current organizational structure, with particular focus on warfighting capabilities, and what modifications—if any—do you think are necessary to the current organizational structure, including any Goldwater-Nichols Act provisions?

Recently enacted reforms and the coming elevation of U.S. Cyber Command (USCYBERCOM) to a full Combatant Command with expanded acquisition authorities directly address the fundamental challenges – the need for a much faster pace of development of advanced warfighting capabilities coupled with feasible acquisition and sustainment cost. This is critical in cyber and I believe we now have the organizational opportunity needed to do so. I am optimistic about these changes and do not see any need for further adjustments at this time.

Duties and Qualifications

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

The Commander, USCYBERCOM is responsible for the planning and execution of the cyberspace missions specified in Section 20.b.(1) of the Unified Command Plan (UCP), as directed, to secure our Nation's freedom of action in cyberspace and to help mitigate risks to our national security resulting from America's growing dependence on cyberspace. In coordination with mission partners, specific missions include: directing Department of Defense information network (DoDIN) operations; securing and defending the DoDIN; maintaining freedom of maneuver in cyberspace; executing full-spectrum military cyberspace operations; providing shared situational awareness of cyberspace operations, including indications and warning; integrating and synchronizing cyberspace operations with Combatant Commands and other appropriate U.S. Government agencies tasked with defending our Nation’s interests in cyberspace; and providing support to civil authorities and international partners. All these efforts support DoD’s overall mission in cyberspace of defending the Nation against cyber attacks, supporting the Combatant Commands, and defending Department of Defense (DoD) networks.

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 (USD(I)), the Director of the National Security Agency (NSA) is primarily responsible for ensuring the NSA successfully conducts two principal missions: signals intelligence (SIGINT) collection and information assurance protection. The collection of SIGINT, under Executive Order 12333, provides intelligence on America's adversaries. Through information assurance, conducted primarily under National Security Directive 42, the NSA protects America's vital national security information and systems from theft or damage by others. The Director of the NSA also is the Chief of the Central Security Service, which includes the elements of the armed forces that perform cryptologic activities.

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

For the past ten years, I have been involved in planning, leading, and executing cyberspace operations. I commanded the Cyber National Mission Force, where I led several intrusion response actions against unclassified DoD networks. I currently command Army Cyber Command, where I am responsible for the operations and defense of the Army's unclassified and classified networks, and Joint Force Headquarters-Cyber (Army), which conducts full-spectrum cyberspace operations in support of Joint Force Commanders.

I have served in intelligence positions across Joint and Army forces in peace and war. I understand how to produce timely, accurate, and valued intelligence, and what consumers demand of our intelligence products. Finally, I have served within the National Security Agency on three separate occasions.

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

For over three decades, I served in leadership positions across Joint and Army forces in peace and war. I commanded military personnel at all levels. Currently, I command Army Cyber Command, Joint Force Headquarters-Cyber (Army), and Joint Task Force-ARES, which is focused on conducting offensive cyberspace operations against ISIS.

My service has included formative assignments with the Joint Staff, Multi-National Forces Iraq, U.S. Forces Afghanistan, and USCYBERCOM. These experiences have afforded me significant insight into command and leadership at the strategic, operational, and tactical levels, with broadening exposure to the interagency, coalition partners, commercial industry, and academia.

Finally, I have attended a series of schools and participated in educational experiences to prepare for leadership at the most senior levels of our military.

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?

If confirmed, I would look to enhance my expertise by visiting our mission partners and key customers. I am also a firm believer in life-long learning, including a continual need to read, study, and write on a variety of topics. If confirmed, 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, and cybersecurity.

Relationships

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

Pursuant to title 10, U.S.C., section 164, and subject to the direction of the President, the Commander, USSTRATCOM 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. As a sub-unified command under the authority, direction, and control of the Commander, USSTRATCOM, USCYBERCOM is responsible to the Secretary of Defense through the Commander, USSTRATCOM. If confirmed, I will work closely with the Secretary in coordination with the Commander, USSTRATCOM.

The Deputy Secretary of Defense

Pursuant to title 10, U.S.C., section 132, the Deputy Secretary of Defense performs such duties and exercises 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, in coordination with the Commander, USSTRATCOM.

The Director of National Intelligence

The Intelligence Reform and Terrorist Prevention Act of 2004 established the Director of National Intelligence to act as the head of the Intelligence Community and as principal advisor to the President and the National Security Council on intelligence matters pertaining to national security, and to oversee and direct the implementation of the National Intelligence Program. Pursuant to title 50, U.S.C., section 403, subject to the authority, direction, and control of the President, the Director of National Intelligence coordinates national intelligence priorities and facilitates information sharing across the Intelligence Community. If confirmed, I will work closely with the Under Secretary of Defense for Intelligence (USD(I)), in coordination with the

Commander, USSTRATCOM as appropriate, to ensure responsiveness to the Director of National Intelligence in the exercise of his authorities.

The Under Secretary of Defense for Policy

As the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary of Defense, the Under Secretary for Policy formulates national security and defense policy, integrates DoD policy and plans, and performs oversight of defense policy goals to achieve national security objectives. If confirmed, I look forward to working closely with the Under Secretary of Defense for Policy, in coordination with Commander, USSTRATCOM, on all policy issues that affect USCYBERCOM operations.

The Under Secretary of Defense for Intelligence

The USD(I) 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) exercises authority, direction, and control on behalf of the Secretary of Defense over the National Security Agency / Central Security Service. If confirmed, I look forward to working closely with the USD(I), in coordination with Commander, USSTRATCOM, on matters in the area of USCYBERCOM's assigned responsibilities.

The Under Secretary of Defense for Acquisition and Sustainment

The Under Secretary of Defense for Acquisition and Sustainment is the senior procurement executive for the Department of Defense, with the mission of delivering and sustaining timely, cost-effective capabilities for the armed forces. If confirmed, I look forward to working closely with the Under Secretary of Defense for Acquisition and Sustainment, in coordination with the Commander, USSTRATCOM, to find ways to acquire and field cyber capabilities more quickly and affordably.

The Under Secretary of Defense for Research and Engineering

The Under Secretary of Defense for Research and Engineering is the chief technology officer of the Department of Defense, with the mission of advancing technology and innovation for the armed forces. If confirmed, I look forward to working closely with the Under Secretary of Defense for Research and Engineering, in coordination with the Commander, USSTRATCOM, 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

The Assistant Secretary of Defense for Homeland Defense, under the authority, direction, and control of the Under Secretary of Defense for Policy, executes responsibilities including overall supervision of the homeland defense and Defense Support of Civil Authorities (DSCA) activities of the DoD. If confirmed, I look forward to working with the Assistant Secretary of Defense for Homeland Defense, in coordination with the Commander, USSTRATCOM and the Under Secretary of Defense for Policy, on matters in the area of USCYBERCOM's assigned responsibilities.

The Chief Information Officer

Under the authority of Department of Defense Directive 5144.02 and consistent with Titles 10, 40, and 44, U.S.C., 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 workforce, for nuclear command and control systems, positioning, navigation and timing. Additionally, the CIO exercises authority, direction, and control over the Defense Information Systems Agency. If confirmed, I look forward to working closely with the Chief Information Officer, in coordination with the Commander, USSTRATCOM, on matters in the area of USCYBERCOM's assigned 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. Title 10, U.S.C, Section 163 allows communication between the President or the Secretary of Defense and the Combatant Commanders to flow through the Chairman. By custom and tradition, and as instructed by the Unified Command Plan, if confirmed, I would normally communicate with the Chairman in coordination with the Commander, USSTRATCOM.

The Secretaries of the Military Departments

Pursuant to title 10, U.S.C., section 165, subject to the authority, direction, and control of the Secretary of Defense, and subject to the authority of the Combatant Commanders, the Secretaries of the Military Departments are responsible for administration and support of forces that are assigned to unified and specified commands. The authority exercised by a sub-unified combatant commander over Service components is clear but requires coordination with each Secretary to ensure there is no infringement upon those lawful responsibilities which a Secretary alone may discharge. If confirmed, I look forward to building a strong and productive relationship with each of the Secretaries of the Military Departments, in partnership with the Commander, USSTRATCOM.

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, in partnership with Commander, USSTRATCOM.

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

USCYBERCOM is a subordinate unified command under USSTRATCOM. 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 planning, leading, and conducting DoD defensive cyber and global network operations and, in general, is a supporting commander for offensive missions. Specific relationships with the Commander, U.S. Northern 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, in coordination with the Commander, USSTRATCOM, to broaden and enhance the level and range of these relationships.

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. Commander, USCYBERCOM must maintain a close relationship with the DISA Director, to coordinate and represent requirements in this mission area, in order to accomplish USSTRATCOM-delegated UCP missions. If confirmed, I look forward to working closely with the DISA Director on matters of shared interest and importance.

Major Challenges and Priorities

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

The next Commander of USCYBERCOM will face three major challenges: a growing variety of threats from nation-state, non-state, and unaligned actors; continued integration of cyberspace capabilities to support Joint / Combatant Commanders in conflict today and into the future; and the establishment of a new Combatant Command, with distinct responsibilities.

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?

The next Director of the National Security Agency (NSA)/Chief of the Central Security Service (CSS) will face continued challenges to the intelligence collection mission given rapid technological evolution, ubiquitous encryption, and the growing capabilities of the private-sector technology industry; and ensuring continued network security from both external and internal threats; and the continuing organizational development given the NSA 21 initiatives.

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

If confirmed, I would focus on: (1) Transitioning USCYBERCOM from building forces to developing increasingly ready and capable cyber forces, (2) Continuing improvements to support Joint / Combatant Commanders with cyberspace capabilities, and (3) Ensuring the rapid transition of the command to fulfill broader Combatant Command responsibilities.

If confirmed as Director of the NSA/Chief of the Central Security Service, I would focus on: (1) Talent—determining how the NSA can better retain its best and brightest, (2) Technology and Innovation—fostering a culture that enables critical leap-ahead capabilities, and (3) Targets—developing partnerships and efforts to gain deep presence in our adversaries' networks to enable insights for policymakers and warfighters.

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

If confirmed, my priorities for USCYBERCOM will be to increase readiness across our cyber mission force; promote interagency, coalition, and industry partnerships; and assumption of broader Combatant Command responsibilities.

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

If confirmed, my priorities for the NSA/CSS will be to recruit and retain top talent, improve signals intelligence (SIGINT) collection against critical adversaries, and ensure the security of NSA's network and enterprise.

Relations with Congress

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 interaction with the Senate Armed Services Committee (SASC). Members of the SASC have been very supportive of USCYBERCOM through office calls, round table briefings, hearings and visits. Additionally, the SASC professional staff members (PSM) have supported USCYBERCOM via meetings, attendance at conferences, and staff delegations. These efforts help build relationships and ensure a common understanding of cyber to include capabilities, threats, authorities and mission execution. If confirmed, I look forward to continuing this relationship.

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, including informing Congress on the Command's activities and, when requested, make myself available to answer questions and provide testimony. I will ensure compliance with the FY18 National Defense Authorization Act (NDAA). I will work to maintain the close relationships with Members on the SASC and ensure my Legislative Liaison office continues to work with the PSMs and personal staff members.

Torture and Enhanced Interrogation Techniques

Do you support the standards for detainee treatment specified in the revised Army Field Manual on Interrogations, FM 2-22.3, issued in September 2006, and in DOD Directive

2310.01E, the Department of Defense Detainee Program, dated August 19, 2014, and required by section 1045 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92)?

Yes.

Cyber Threats

In your view, what are the most serious cyber threats facing the United States today?

Cyber vulnerabilities in the private sector and especially in the defense industrial base pose a serious threat to U.S. national security. As military defenses are relatively formidable, critical infrastructure and the defense industrial base and private sector are likely seen as a rich source of information and a critical vulnerability in the Nation's armor. State actors have therefore demonstrated the capability and willingness to target and gain access to U.S. businesses as well as federal, state and local governments. The magnitude of data exfiltration from both industry and government is just as serious as the military espionage aimed at reducing our technical advantages against our adversaries. Cyber criminals and non-state actors also pose concerns.

What future strategic 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. Cyber threats are already challenging public trust and confidence in global institutions, governance and norms, and are imposing significant costs on the U.S. and global economies. Cyber threats also pose an increasing risk to public health, safety and prosperity as cyber technologies are integrated with critical infrastructure in key sectors. Adding to the problem, some adversaries remain unconstrained from conducting reconnaissance, espionage, influence and even attacks in cyberspace. Additionally, the U.S. should closely monitor and prepare for threats utilizing emerging technologies such as artificial intelligence and machine learning.

What are your views on Russia's cyber capabilities?

As the most technically advanced potential adversary in cyber space, Russia is a full-scope cyber actor, employing sophisticated cyber operations tactics, techniques and procedures against U.S. and foreign military, diplomatic, and commercial targets, as well as science and technology sectors. Russia will likely continue to integrate cyber warfare into its military structure to keep pace with U.S. cyber efforts, and conduct cyberspace operations in response to perceived domestic threats. Also, Russian cyber actors' have demonstrated the intent and capability to target industrial control systems found in the energy, transportation and industrial sectors.

What are you views on China's cyber capabilities?

I consider China a strategic competitor, whose cyber capabilities pose a high threat to U.S. government and commercial networks. China is using its cyber capabilities to support intelligence collection against U.S. diplomatic, economic, and defense industrial base targets important to U.S. national security. The information targeted could potentially be used to benefit China's defense industry and high technology industries. China is one of many states seeking to integrate cyberspace operations into their traditional military capabilities, while also mounting a sustained campaign to pursue our technology and weapon systems as they are developed by cleared defense contractors. China is a near-peer competitor in cyberspace.

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

I believe North Korea poses a moderate cyber threat to U.S. government and commercial networks, and has already demonstrated the willingness to target U.S. infrastructure as evidenced by its 2014 cyberattack on Sony Pictures. North Korea uses its cyber capabilities as a cost-effective and deniable asymmetric tool to finance the regime and to pursue its national objectives on a global scale.

What are you views on Iran's cyber capabilities?

Iran is a mid-level cyber actor that will almost certainly remain a pervasive cyber threat to the U.S., particularly as it puts additional emphasis on its cyber program. Domestically, Iran uses its capabilities to help control the country's population and shape the narrative that reaches the Iranian people. Outside the country, Iran very likely considers its cyber program as an important tool in carrying out asymmetric retaliation against adversaries and to gather intelligence to support national and military objectives.

What are you views on transnational terrorist groups' cyber capabilities?

Transnational terrorist groups' threats in cyberspace are largely limited to nuisance activities. These groups continue to leverage resources to develop online media capabilities and they continue to research and implement secured communication methods in cyberspace. Transnational terrorist groups' cyber operations against the DoDIN and U.S. critical infrastructure / key resources are limited to website defacements, and the collection and posting of publicly available service member and civilian personally identifiable information (PII). Most of these activities are accomplished through unsophisticated cyber operations with limited or isolated effects. However, that assessment could change and this is an area I will continue to assess over time, if confirmed.

Who are our most capable cyber adversaries?

Russia and China remain the most prolific and capable cyber adversaries while Iran and North Korea are continuing to mature their capabilities to target national security interests.

Are the cyber attacks targeting the United States increasing in severity, sophistication, or frequency? If so, why is this the case?

Yes. A relatively unsophisticated cyber attack can significantly disrupt a poorly defended system. Our adversaries likely assess there are minimal consequences in response to their malign actions and are increasingly devoting resources to their cyber programs resulting in increased sophistication and frequency of their cyber operations. It is paramount that the U.S public and private sectors work together to create a shared understanding of the threat in order to better defend our national security interests.

What steps do you believe the Department of Defense should take to reduce the frequency and severity of cyber intrusions from the governments of China and Russia? What about other cyber adversaries?

With threats to our critical information constantly evolving, we need to explore avenues in policy and regulation to outpace our competitors and adversaries. Enforcement of existing policies and contract requirements is the first step. The Department of Defense (DoD) relies on its industry and corporate partners to provide key services and resources; DoD assistance to private industry is based on consent, so it is essential that we continue developing these partnerships and working relationships for our mutual benefit.

U.S. Cyber Command Missions

In an overarching sense, how do you define the U.S. Cyber Command mission?

In line with the Secretary of Defense's 18 August 2017 memorandum, I would define USCYBERCOM's mission as directing, synchronizing, and coordinating cyberspace planning and operations, to defend and advance national interest in collaboration with domestic and international partners.

How do you define the roles of the National Mission Teams?

Ready, postured, and in place with full spectrum operational capabilities to defend the Nation against specified adversaries and threats in, from, and through cyberspace, as directed.

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 threat priorities identified in the National Defense Strategy?

No, not at this time. I do, however, believe the National Defense Strategy will inform existing processes to prioritize and allocate cyber forces.

How successful has U.S. Cyber Command been at integrating its national defensive, national offensive, and command support missions and acquiring the expertise needed to perform them?

USCYBERCOM is effectively integrating and continually maturing its capabilities for defense, offense and support to Joint Force Commands. The work by the Office of the Secretary of the Defense (OSD), Joint Staff, and Services over the past seven years has enabled the Department to recruit and build the force on schedule, to acquire the tools and infrastructure, and establish the mission management capabilities, required to effectively employ the force. USCYBERCOM will complete its "build" phase by the end of June 2018, ahead of the mandated 30 September 2018 completion date. The new Integrated Cyber Center-Joint Operations Center is on track to meet full operational capability (FOC) in July 2018, and the impending elevation of USCYBERCOM to a Combatant Command will significantly increase its capabilities. If confirmed, I will aggressively work to ensure we maintain our most important capability—a highly trained and motivated work force.

What organizational challenges remain at U.S. Cyber Command related to its missions? Specifically, what additional work, if any, remains to be done and what expertise, if any, needs to be acquired for these missions?

As USCYBERCOM matured its capabilities and increased its operations it became evident that a more robust command and control structure was required to better support Joint Force Command requirements. To address this challenge DoD approved the creation of Joint Force Headquarters-Cyber (JFHQ-C) for each Service Cyber Component and a Cyberspace Operations Integrated Planning Elements (COIPE) at each Combatant Command. This additional capability provides a robust and responsive capability for full spectrum cyberspace operations at the Combatant Commands and offers significant advantage if resourced and implemented effectively. To fully recognize the benefits of elevating USCYBERCOM to a Combatant Command requires that we must build a more effective and robust team enabling us to enhance our partnership with service component, interagency, and foreign partners. USCYBERCOM’s continued special relationship with the intelligence community, particularly NSA, will enhance our ability to achieve mission success. Even if a decision is made to terminate the NSA/ USCYBERCOM dual-hat, an exceptionally close and collaborative relationship is essential as this is the foundation of our success. This is an area I will be assessing aggressively, if confirmed.

If confirmed, would you recommend or support any changes in the missions currently assigned to U.S. Cyber Command? If so, what changes would you recommend?

The Defense Department is currently in the process of elevating USCYBERCOM to full Combatant Command status. If confirmed, this is an area that I will spend time assessing. I will then make recommendations as appropriate.

Are you aware of any additional new missions that are being contemplated for U.S. Cyber Command?

I am not aware of any other than the planned elevation to full Combatant Command status.

National Security Agency (NSA) Missions

In an overarching sense, how do you define the NSA mission?

NSA's mission is to apply the capabilities of Signals Intelligence (SIGINT) to generate maximum insights in the areas of foreign intelligence and cyber security in the defense of our Nation and our friends and allies around the world within our Nation's legal framework and applicable policy guidance. NSA executes that mission at all times within the rule of law, while respecting the rights and privacy of our citizens.

In an overarching sense, how do you define the NSA mission as it relates to cyber?

NSA’s mission as it relates to cyber is twofold. First, NSA is responsible for securing national security systems, which includes systems relating to military or intelligence activities or those that handle classified information. Second, NSA has a responsibility to use cyber means, including cyberspace operations, to obtain foreign intelligence information.

What role does the NSA play in support of U.S. Cyber Command?

As an intelligence organization and a Combat Support Agency (CSA), NSA plays a significant role in generating insightful, timely and relevant intelligence that supports operational commanders like USCYBERCOM. Given its strong focus and role in cyber security, NSA has a particularly significant role to play in support of USCYBERCOM's mission.

A January 2, 2018 article in the *Washington Post* titled, "NSA's top talent is leaving because of low pay, slumping morale and unpopular reorganization," suggests that the NSA is losing talent at a "worrisome rate," as personnel have become disillusioned with the NSA's leadership, reorganization, and compensation. Do you have any concerns regarding the NSA's work climate?

Mindful that what one reads in the press not always accurate, anytime I am joining a new organization I am going to assess the work climate and how I can be a part of improving that climate. If confirmed, one of my top priorities upon taking the job will be assessing the state of the NSA workforce, including morale and work climate and ensuring we are employing, empowering, and retaining the best and brightest talent our Nation has to offer.

Do you plan to reevaluate any of the organizational changes that occurred as a result of NSA21?

NSA is a large agency with many employees and components. If confirmed, I will be looking for any opportunity to innovate and improve organization and functions to best support the mission and meet the ever-changing threat landscape. However, organizational changes need time to mature. NSA21 has just reached full operational capability. I am not inclined to rush toward further change before better understanding current effectiveness.

Do you plan to reevaluate the NSA's moratorium on "upstream" or "about" surveillance of foreign targets as announced in an April 28, 2017 NSA press release?

As with all operational decisions, I cannot fully assess this fact-specific question unless I am fortunate enough to be confirmed. Operational decisions such as these will depend on the threat landscape, technology, and other resources available; the compliance costs and controls associated with the outcomes; and the policy direction as well as the law.

Do you believe that any of the mass or narrow surveillance capabilities currently employed by the NSA demand reconsideration or adjustment?

As with all operational decisions, I cannot fully assess this fact-specific question unless I am fortunate enough to be confirmed. I also note that NSA operational decisions are made with the goal of meeting requests made by policy makers through the National Intelligence Priority Framework.

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

I believe NSA has made significant strides over the last several years in an effort to be more transparent about its mission and activities. There is always room for improvement; however, I am mindful that our adversaries can and do monitor what information NSA releases in order to secure every advantage possible against our Nation.

What steps can be taken to improve relations between the NSA/U.S. Cyber Command and the private sector, especially companies in Silicon Valley?

There are natural overlapping interests that will continue to serve as the basis for our relationship with the private sector. For example, we both rely on the same cyber infrastructure. Beyond the practical bonds, we share many core values as Americans, which I believe is a solid foundation to build upon.

Combat Support Agency

In an overarching sense, how do you define the role of a combat support agency?

A Combat Support Agency (CSA) is one that fulfills support functions for 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 establishing directives and pertinent DoD planning guidance.

What are the NSA's prerogatives as a combat support agency distinct from U.S. Cyber Command?

The relationship between a CSA and a Combatant Command is support, as defined in Joint Publication 1, "Doctrine for the Armed Forces of the United States," 25 March 2013, with the CSA typically operating in a supporting-to-supported relationship to the Combatant Commanders. NSA is a Defense Agency with intelligence and cybersecurity missions, and its combat support typically relates to these activities. USCYBERCOM is a sub-unified command, with a mission to plan and execute global cyberspace operations as directed.

Do you anticipate that the NSA will increasingly serve as a combat support agency vice conducting cyber operations, irrespective of the dual-hat decision?

I expect both roles will continue irrespective of the dual-hat decision. NSA's ability to provide combat support, whether in the manner of providing foreign intelligence information or cyber security assistance, is informed by NSA's cyber operations.

When was the last review of the roles and responsibilities of the NSA as a combat support agency conducted?

The Joint Staff J8's 2017 Combat Support Agency Review Team (CSART) conducted their biennial assessment of NSA/CSS from January 2017 - September 2017. This report highlights findings, issues, and provides recommendations for the DIRNSA to implement.

Act of War in Cyberspace

What do you believe would constitute an act of war in cyberspace?

International law prohibits the use of force or armed attacks by states except as a matter of self-defense or with the authorization of the UN Security Council. These international rules apply fully to cyberspace. As in the physical domains, it is generally accepted that cyber operations that cause death, injury, or significant damage to property would likely be considered a prohibited use of force triggering the U.S.'s inherent right of self-defense. Ultimately, the determination of what constitutes an unlawful armed attack is fact-dependent and assessed on a case-by-case basis. It is important to note that malicious cyber operations that do not clearly cross these international law thresholds may nonetheless constitute violations of other norms of international law and trigger appropriate response options.

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

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

The Department of Defense fights and wins the Nation's wars while defending the homeland from external threats abroad. DoD through USCYBERCOM and NSA, serves as part of a larger Executive branch team that works together to defend the Nation from malicious cyber activity, including cyber attacks. I see USCYBERCOM and NSA as developers and key integrators of capabilities to deliver effects that deter adversaries from conducting attacks of significant consequence against the U.S. They collaborate extensively with the Department of Homeland Security (DHS) and the Department of Justice (DOJ)/Federal Bureau of Investigation (FBI) to effectively employ each of their distinct authorities and capabilities to defend the Nation from attacks in cyberspace.

Deterrence

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

Do you anticipate that the Nation's and military's exposure in cyberspace is increasing?

Yes. All elements of our society, now depend on reliable and rapid flows of accurate digitized information, and continue to infuse technology and interconnectivity into all activities. This has created both opportunities and vulnerabilities.

Do you agree with the principal findings of the 2017 Defense Science Board Task Force on Cyber Deterrence? What is the Department and U.S. Cyber Command doing to implement the recommendations of the Task Force?

Yes. The principal findings of the Defense Science Board (DSB) Task Force on Deterrence were the need for tailored deterrence campaigns; increased cyber resilience; and improved attribution.

I agree that a one-size approach will not fit all U.S. adversaries, and that deterrence planning must be integrated with broader political-military campaigns tailored to each potential adversary. USCYBERCOM has undertaken an aggressive planning effort recommended by the DSB, focusing on the most likely attacks and the most dangerous risks. I agree that improved cyber resilience is necessary and, if confirmed, will seek to improve the resilience of systems and platforms, as well as preparing our forces to operate in a degraded environment.

Do you believe that deterrence is possible in cyberspace? Is the current level and tempo of cyber attacks on the Department and on the Nation tolerable?

I believe it is possible for actions in cyberspace to have a deterrent effect and contribute to the Nation's overall deterrence posture. Effective deterrence requires a whole-of-government approach, however, and cannot rely solely on efforts in cyberspace.

The current level and tempo of cyber attacks is not tolerable. Our adversaries see opportunity for strategic advantage through continuous activity in the domain. We must act purposefully to frustrate their intentions, increase their costs, and decrease their likelihood of success.

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

DoD can contribute more effectively to the Nation's overall deterrence posture by continuing to build the operational expertise and capacity necessary to meet growing cyberspace threats and counter cyber aggression before it reaches our networks and systems. To do so, we must ensure that policies to employ these capabilities allow a tempo of operations consistent with the nature of the domain. This is an area in which I believe we must improve.

How can the Department improve its cyber deterrence posture?

The Department can improve its cyber deterrence posture in several ways. First, by conducting operations to frustrate and counter adversary cyber activities to decrease will, increase cost, and deny benefits. Second, by developing a highly skilled force and demonstrating capabilities to deliver cyber effects and hold adversaries at risk. Finally, by improving the defense and resilience of critical systems and infrastructure.

Do you believe that an effective cyber deterrence posture is possible with the Cyber Mission Force's current mix and size?

If properly employed, I believe the Cyber Mission Force (CMF) can effectively deliver effects and generate deterrent effect through tailored campaigns. If confirmed, I intend to assess the CMF's effectiveness in order to determine whether adjustment to force mix, size and employment are warranted.

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

If confirmed, this is an area that I will spend time assessing. I will then make recommendations as appropriate.

Does the Department defer excessively to the concerns and policy positions of other actors in the interagency? Does this impede its stand-up of its deterrence posture?

The Department operates as part of an interagency team. Whole-of-government approaches for protecting, defending, and operating in cyberspace can benefit from the insights of USCYBERCOM, which operates daily in cyberspace against capable adversaries, and retains significant capacity for planning and synchronizing. We strive to work as one team, but need to enhance and integrate efforts to enable each other and build the U.S. Government's cyber enterprise to achieve the Nation's goals.

Dual Hat

The Trump Administration is currently in the process of evaluating whether the separation of the U.S. Cyber Command-NSA "dual hat," apparently on course during the last administration, would be wise at this time.

What is your position on maintaining the "dual hat" relationship where the Commander of U.S. Cyber Command is also the Director of the NSA, now and in the future?

My position on the "dual-hat" relationship is that any decision must be conditions-based and in the best interests of the Nation. The 2017 NDAA identified six conditions required for terminating the dual-hat arrangement. If confirmed, I will evaluate these conditions and provide my assessment to the Secretary of Defense and the Chairman of the Joint Chiefs of Staff, who must certify these conditions are met to ensure that termination does not adversely impair either organizations' mission.

Do you believe that a single leader of both organizations is compromised by the organizations' differing missions or that this unified leadership enables more efficient navigation of these differing missions?

No, I do not believe a single leader is compromised by the organizations' differing missions. My experience is that the dual-hat arrangement has enabled the operationally close partnership between USCYBERCOM and the NSA, which benefits both in the accomplishment of their respective missions.

What are the risks of premature separation?

If confirmed, I will better be able to assess the risks of premature separation. Terminating the "dual-hat" relationship prior to the Secretary of Defense and the Chairman of the Joint Chiefs of Staff certification of the 2017 NDAA conditions have been met entails significant risk, including the possibility that processes and policies for effective coordination and deconfliction between USCYBERCOM and NSA will not be in place, thereby reducing the speed and agility of cyber operations. Other premature separation risks include the potential for reduced cohesion between USCYBERCOM and NSA and the potential disruption of resources currently available for USCYBERCOM to effectively accomplish its mission.

What are the risks of the maintenance of the status quo?

If confirmed, I will better be able to properly assess the risks of maintaining the status quo. The economies of scale currently enjoyed under the dual-hat arrangement will no longer remain necessary once the 2017 National Defense Authorization Act conditions are met. Failure to split at the proper time might create an environment where neither USCYBERCOM nor NSA are taking on as many challenges related to their respective missions as they might otherwise.

Where is the Department in ensuring that the conditions laid out in section 1642 of the National Defense Authorization Act for Fiscal Year 2017 are met prior to a hypothetical separation of the dual hat? Is progress being made towards these conditions irrespective of the ultimate decision whether to separate?

The Office of the Secretary of Defense and Joint Staff are leading the effort to assess the status of the conditions specified in section 1642 of the 2017 NDAA. In addition, the Chairman of the Joint Chiefs of Staff has issued three planning orders directing USCYBERCOM and the NSA to provide detailed courses of actions and risk mitigation measures necessary for terminating the dual-hat arrangement. Progress is being made towards these conditions irrespective of the ultimate decision. For example, the CMF will achieve full operational capability regardless of the ultimate decision.

Does the Department maintain conditions beyond these legislative requirements? What progress is being made towards meeting these?

I am not aware of any additional conditions maintained beyond those specified in the 2017 NDAA. However, if confirmed, I will look at the need for mutual support agreements between USCYBERCOM and NSA in order to mitigate any potential risk resulting from termination of the relationship.

<u>Elevation</u>

In the fall of 2017, the Trump Administration announced that the elevation of U.S. Cyber Command to status as a full unified combatant command was imminent.

How do you plan to balance the priorities of the other combatant commands and their mission support requirements from U.S. Cyber Command with its national offensive and defensive missions?

In 2017, USCYBERCOM executed its first major realignment of the CMF since 2012 to address both national level and Combatant Command requirements. The key to this successful effort was continual engagement with the Combatant Commands and other stakeholders to ensure decisions to align the force and balance risk were well understood. Further, clear prioritization based on national level guidance and adversary activity is essential to effectively employing USCYBERCOM's high demand/low density force in a manner that supports both national and Combatant Command intent. To that end, if confirmed, I will continue to use and refine collaborative forums, including Combatant Commands, Service and DoD Agency participation, to balance cyberspace operations requirements with the limited force available.

Is U.S. Cyber Command currently equipped and manned to carry out these missions simultaneously?

Yes. I believe that USCYBERCOM is equipped and manned to perform those missions simultaneously. If confirmed, this is an area that I will carefully assess.

Do you anticipate that U.S. Cyber Command's independence will improve its prioritization and execution of its national offensive and defensive missions?

Yes. Elevation enables input directly into foundational DoD processes; increases decision speed between the Commander, Chairman of the Joint Chiefs, Secretary of Defense, and President; aligns responsibility, authority, situational awareness, and capability under a single, dedicated Combatant Commander; and raises and aligns resource advocacy for the prioritization and allocation of resources.

Focus on Intelligence Gathering versus Focus on Warfighting

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, has very different interests and objectives. For example, it must have the capability to act rapidly, it may need tools and processes that do not require computer scientists to operate them, and it may need to act in a fashion that makes it clear that a given operation is an attack by the United States.

Do you believe that you could direct U.S. Cyber Command wartime operations effectively if U.S. Cyber Command were only able to use the NSA's infrastructure and tools to support those operations?

No. Operating under the constraint of the intelligence authorities that govern NSA infrastructure and tools would severely limit USCYBERCOM's ability to effectively support wartime cyber operations.

How scalable are the NSA's infrastructure, personnel, and tools for supporting combat operations in cyberspace?

NSA uses its infrastructure, personnel, and tools to support combat operations in cyberspace and will continue to do so regardless of whether NSA and USCYBERCOM split. Given adequate funding, NSA's assets can scale to meet the demand placed on the agency to support combat operations in cyberspace. Additionally, the Department is properly investing in building USCYBERCOM's own organic abilities to support combat operations. To most effectively manage risks across military and intelligence operations in cyberspace, USCYBERCOM and the Services have leveraged NSA expertise to build cyberspace capabilities for combat operations which include additional tools and infrastructure that are unique and distinguishable from those of the intelligence community.

On what schedule should U.S. Cyber Command develop the capability to take offensive actions that do not require hiding the fact that the operations are being conducted by U.S. forces?

USCYBERCOM currently conducts operations in cyberspace against our adversaries that do not require hiding the fact that they are being conducted by U.S. forces.

Hollow Force

The Services are primarily responsible for the construction and maintenance of the Cyber Mission Force and its achieving Full Operation Capability. Unfortunately, spending and attention deficits have threatened the technological capacity of that force.

Is the Department of Defense on track to meet the Full Operational Capability targets for the training of the Cyber Mission Force in the fall of 2018?

Yes. Only four teams remain at initial operational capability (IOC). I expect the CMF will achieve fully operational capability (FOC) by 30 June 2018—ahead of the mandated 30 September 2018 deadline.

Has the Department specified the materiel, command and control, doctrine, operational concepts, and TTPs requirements—that is, the non-personnel and personnel training capabilities—necessary for the Cyber Mission Forces to be operationally capable? Is the Department on track to meet the Full Operational Capability targets for hardware, software, and weaponry for the Cyber Mission Force in the fall of 2018?

The DoD has fully addressed and resourced all elements required for the Cyber Mission Force (CMF) needed to meet all FOC targets. As of this month, only four teams have not yet reached FOC status, and they are on path to achieve this by 30 June 2018 ahead of the mandated 30 September 2018 deadline. That being said, the Department does not see FOC criteria as the desired end-state of CMF capability. As we actively employ these Teams in operations, we continue to mature our understanding of how to strengthen the mission readiness of this force. The Department has made significant investments in cyber payloads and toolsets for the CMF, a formal study is currently underway to more comprehensively inform requirements based on lessons learned from recent operations.

Has the Army made the requisite investments to ensure that its cyber operators have the tools and weapons required to defend and fight in cyberspace?

Yes. I believe the Army has made and continues to make the requisite investments in infrastructure, accesses, and cyber tools for its 41 CMF teams to defend and fight in cyberspace.

Has the Navy made the requisite investments to ensure that its cyber operators have the tools and weapons required to defend and fight in cyberspace?

My understanding is that the Navy has made and continues to make the requisite investments to ensure its 40 CMF teams can defend and fight in cyberspace.

Has the Air Force made the requisite investments to ensure that its cyber operators have the tools and weapons required to defend and fight in cyberspace?

My understanding is that the Air Force has made and continues to make the requisite investments to ensure its 39 CMF teams can defend and fight in cyberspace.

Has the Marine Corps made the requisite investments to ensure that its cyber operators have the tools and weapons required to defend and fight in cyberspace?

My understanding is that the Marine Corps has made and continues to make the requisite investments to ensure its 13 CMF teams can defend and fight in cyberspace.

Is the Cyber Mission Force, as it currently stands and as it is projected, manned sufficiently to carry out its offensive and defensive missions?

Yes. However, I believe the challenge across all Services is the training and retention of highly skilled personnel.

Has the Army made the requisite investments in personnel to ensure that it has the capacity and expertise to sustain readiness and defend and fight in cyberspace?

Yes. The Army established a cyber career field, built a school to educate and train its force, and is leveraging the direct hiring and direct commissioning authorities provided by Congress.

Has the Navy made the requisite investments in personnel to ensure that it has the capacity and expertise to sustain readiness and defend and fight in cyberspace?

My understanding is that Navy has made and continues to make the requisite investments in personnel, specifically in recruiting, training and retaining those with the expertise required to defend and fight in cyberspace.

Has the Air Force made the requisite investments in personnel to ensure that it has the capacity and expertise to sustain readiness and defend and fight in cyberspace?

My understanding is that Air Force has made and continues to make the requisite investments in personnel, specifically in recruiting, training and retaining those with the expertise required to defend and fight in cyberspace.

Has the Marine Corps made the requisite investments in personnel to ensure that it has the capacity and expertise to sustain readiness and defend and fight in cyberspace?

My understanding is that the Marine Corps has made and continues to make the requisite investments in personnel, specifically in recruiting, training and retaining those with the expertise required to defend and fight in cyberspace. The Marine Corps also recently approved a new cyberspace military occupational specialty (MOS) that will help address the readiness and retention of qualified Marines within the cyberspace community.

Is the current balance between offensive, defensive, and support teams apposite? Are there established processes (or plans) to recalibrate this mix?

The current balance between offensive, defensive and support teams is an initial starting point. The Army has already begun building 21 additional defensive teams in the Army National Guard and Army Reserve. Currently, I know of no other plans to recalibrate this mix of teams. If confirmed, I intend to look at the overall size of the force and its balance of offensive, defensive, and support teams.

Rapid and Efficient Acquisition

Because cyber systems demand bespoke capabilities to surveil, attack, and defend computer networks, rapid acquisition of these capabilities is of the utmost importance. The Department of Defense's traditional methods for acquisition and procurement are woefully ill-equipped to handle this challenging task.

Section 1642 of the National Defense Authorization Act for Fiscal Year 2018 mandated that U.S. Cyber Command evaluate and report on "Agile" iterative approaches to capability development. What are your views on the adoption of Agile acquisition approaches for the development of cyber capabilities?

I support the Agile approach to cyber capability development and support the Department transitioning from its traditional development process toward a more responsive and flexible approach. In today's cyber environment, the traditional acquisition model delivers a solution to a problem too late to be operationally impactful. I believe we need to adopt an evolutionary capability development process, leveraging smaller dollar, cost-type contracts that focus on the rapid delivery of capabilities in weeks versus months or years.

How can the Department improve its commercial acquisition of offensive and defensive capabilities?

One way the Department can improve its commercial acquisition of offensive and defensive cyber capabilities is to fully utilize Other Transaction Authority, which has been delegated to USCYBERCOM. These contract vehicles will enhance the ability to rapidly deliver prototypes to the CMF. Another possibility is the use of multiple, long-term, Indefinite Delivery, Indefinite Quantity (IDIQ) contracts that allow flexibility and responsiveness to mission needs as they arise. Additionally, USCYBERCOM's Partnership Intermediary Agreements (PIA) expose USCYBERCOM to innovative technologies and capabilities emerging from small businesses and academia, increasing the pace at which USCYBERCOM can deliver capabilities in support of cyber operations.

How can the Department accelerate its indigenous creation and acquisition of offensive and defensive capabilities?

The Department can accelerate the indigenous creation and acquisition of offensive and defensive cyber capabilities by increasing the size and experience level of the cyber workforce. Internal development capabilities are paramount to achieve success at executing the cyber mission. Developing a workforce that is highly skilled and on the cutting edge of technology is a primary objective; however, recruiting and retention remain a challenge. Additionally, the development of a robust military training pipeline for cyber developers would enhance the baseline knowledge level of new arrivals and increase the speed in which they become fully capable members of the team. In an asymmetric threat environment, our people are our biggest asymmetric advantage.

Is the Department satisfied with the current mix of internal and external procurement of cyber capabilities?

USCYBERCOM's capability needs are dynamic. The Department continues to assess and evaluate the options for internal and external cyber development and procurement.

Does the Department possess the requisite authorities to rapidly acquire cyber capabilities?

If confirmed, this is an area that I will spend time assessing. I will then make recommendations as appropriate.

Does the Department possess the requisite relationships with private sector entities to rapidly acquire cyber capabilities?

The Department continues to develop relationships with private sector entities to rapidly acquire cyber capabilities through initiatives such as the Defense Innovation Unit, Experimental (DIUx) and the Point of Partnership (PoP).

What lessons can be learned from the Department’s experiences in rapid acquisition, in response to immediate exigencies?

Recently, USCYBERCOM’s efforts to acquire equipment for an urgent cyber mission team requirement reinforced the imperative to have inter-service support agreements in place while continuing to develop working relationships between USCYBERCOM, the Service Cyber Components, and the Joint Staff. USCYBERCOM's maturing Acquisition Division continues to develop its mastery of the roles, responsibilities, and organic acquisition capability between all departments and agencies.

How can the Department improve its transfer of offensive and defensive capabilities, including the communication of vulnerabilities, to and from its NSA, CIA, DHS, and international counterparts?

USCYBERCOM has established cooperative relationships with NSA, CIA, and DHS and, through negotiated program agreements, with partner nations to improve information sharing. The agencies and partners can leverage USCYBERCOM’s cyber capability demonstration venue and expand the transfer of knowledge across agencies and with private industry and academia, as feasible.

Chief Information Officer

Section 909 of the National Defense Authorization Act for Fiscal Year 2018 establishes the Chief Information Officer as the central coordinating authority for Department of Defense

standards for information technology and cyber capabilities and for assessing the development and procurement of these capabilities.

What is your anticipated relationship with the Chief Information Officer in this capacity?

If confirmed, I am committed to a strong USCYBERCOM-NSA-DoD CIO partnership. The CIO is a key partner in the defense of the DoDIN. I think the relationship can be similar to that between Combatant Commanders and PSAs, where policy, strategy, external engagement and guidance emanate from the Department, and the USCYBERCOM Commander executes operations shaped by those policies and guidance. I will ensure that NSA continues in its efforts to provide the DoD CIO with technical advice and assistance on the development of standards, and to continue the development of capabilities in the cybersecurity solutions space. This support will help ensure the security of the Nation and the Department. I think we all recognize there is a necessary feedback loop as well—where our operations, our threat assessment, and our requirements can and must inform the execution of the CIO's roles and responsibilities.

How can U.S. Cyber Command ease or improve the Chief Information Officer's mission in this respect?

I believe that USCYBERCOM must keep the CIO apprised of threats to the DoD information enterprise. Moreover, USCYBERCOM should identify its defensive cyberspace operations requirements to help the CIO engage with industry and design the future architectures for the domain that USCYBERCOM operates and defends.

Do you have any suggestions or reforms that should be considered concerning the Chief Information Officer and its roles in responsibilities concerning cyber? What about electronic warfare?

I am aware that a cross-functional team exists with representation from key stakeholders across the Department, including the CIO and USCYBERCOM, has convened to discuss the CIO's current and potential roles in cyber. The options generated by this team will be presented to the Secretary of Defense for decision. Concerning electronic warfare (EW), the DoD CIO historically has played a significant role in the management of the electromagnetic spectrum management, but not directly in EW capabilities. The cross-functional team examining the CIO's role in cyber is also considering alignment of EW responsibilities within the Office of the Secretary of Defense.

<u>Defense Science Board Task Force on Cyber Deterrence</u>

Former Secretary of Defense Ashton Carter directed the Defense Science Board to establish a Task Force on Cyber Deterrence. The Task Force report in February 2017 concluded that Department of Defense and interagency partners could achieve deterrence in cyberspace by developing capabilities, and demonstrating a willingness to exercise those capabilities to "hold at risk" those things that the leaders of adversary nations hold most dear or value most highly. The Task Force specifically concluded that threatening those things that adversary leaders value most highly would be an appropriate response to Russia's influence campaign conducted primarily through cyberspace to affect the 2016 elections in the United States.

Do you agree that demonstrating to President Putin that we have the capability and will to threaten his sources of power, wealth, and support would improve our ability to deter Russia from sustaining and intensifying its ongoing campaign to manipulate the American electorate?

Yes.

The Task Force also concluded that it is not possible for the foreseeable future to prevent, by cyber defenses, a peer adversary from severely damaging U.S. critical infrastructure if that adversary is determined to do so. The Task Force concluded that it may be possible to prevent lesser adversaries, such as North Korea, from being able to inflict unacceptable damage to critical infrastructure through concerted defensive efforts. The Task Force's logical conclusion is that we must develop credible means for deterring near-peer adversaries from attacking critical infrastructure, including in wartime, and for defending critical infrastructure effectively from less-capable adversaries.

Do you agree that it is necessary for it to be known by peer adversaries that the U.S. has the ability and will to retaliate effectively against the critical infrastructure of peer adversaries in order to deter peer adversaries from attacking U.S. critical infrastructure?

Yes. The ability to respond appropriately and effectively is an essential element of any deterrence strategy.

Is U.S. Cyber Command and the military services actively developing capabilities to threaten the critical infrastructure of peer adversaries?

Yes.

In your opinion, based on experience to date, will the private sector owners of U.S. critical infrastructure voluntarily invest the resources in cyber defenses that are necessary to effectively defend critical infrastructure in the future against cyber attacks by nations such as North Korea and Iran?

In my current assignment I do not have significant experience in this area, but if confirmed I look to be in a better position, by working with the Department of Homeland Security and the Federal Bureau of Investigation, to assess the readiness of the private sector over time.

Is defense of privately-owned critical infrastructure against severe and sophisticated cyber attacks by nation states the responsibility of the private sector or is that a government responsibility?

This issue should not be viewed in a binary manner. We should look to help each other. For example, the Cybersecurity Act of 2015 facilitates the sharing of threat information in a bidirectional manner. While the responsibility for protecting privately-owned networks lies primarily with the system owner, the U.S. Government has the responsibility to defend national interests more broadly.

Integrated Capabilities for Information Warfare

Section 1637 of the National Defense Authorization Act for Fiscal Year 2018 directed that the Secretary of Defense take actions to integrate across all of the Department of Defense's components that have responsibilities for aspects of information warfare in order to achieve integrated strategies, planning, budgeting, and operations for information warfare to counter and deter malign influence operations against the United States and its allies. The legislation required the Secretary to designate a senior official that would exercise the responsibilities and authorities necessary to achieve effective integration and planning. Further, the Secretary is required to direct each combatant command in coordination with interagency partners to develop specific plans and options to counter and deter information warfare by adversaries in their areas of responsibility.

Has the Secretary of Defense directed U.S. Cyber Command and other combatant commands to develop such plans or indicated his intention to do so?

Yes. The Secretary of Defense, through the Chairman of the Joint Chiefs of Staff, has developed an order directing Combatant Commands to plan, conduct, and report globally integrated strategic activities to shape the perceptions, decisions, and actions of relevant actors via the coordinated and thematically-unified operations, activities, relationships, and investments of the Joint Force. This order and the Joint Strategic Capabilities Plan will coordinate the efforts of the Combatant Commands against priority threats

U.S. Cyber Command and its predecessor commands dating back to the 1990s have always been focused on the technical aspects of cyber warfare—the surveillance, attack, and defense of computers and networks—and not on manipulating the content of the information flowing across networks or the perceptions of the personnel owning or using those networks. This "cognitive" dimension of warfare in cyberspace has not been a major element of U.S. Cyber Command's mission and capability development. Likewise, those in the Department of Defense charged with developing policy and plans for, and conducting what are called "psychological," "deception," or military support operations are disconnected from U.S. Cyber Command. In contrast, adversaries like Russia very plainly conduct cognitive information operations through cyberspace by operators who are skilled in both the technical and perception dimensions.

Do you agree with the goal of section 1637 to "re-integrate" the technical and cognitive aspects of information warfare, while recognizing that there are distinctions between cyber warfare and information operations?

Yes, I agree with the intent behind section 1637, but I also feel Information Operations should be conducted in all domains of the operational environment. The Department views cyber as a component of the information environment, which in turn is a component of the larger operational environment.

How would you propose to achieve the necessary level of integration, and changes in U.S. Cyber Command's role, missions, and capabilities to enable U.S. Cyber Command to effectively contribute to countering and deterring information and influence operations against the United States and its allies?

While USCYBERCOM plays an important role in countering and deterring information operations against the U.S., the mission is not solely USCYBERCOM's. As the Army Cyber and JTF ARES Commander, I was able to see how USCYBERCOM effectively conducted cyber operations in support of Combatant Commands to counter and deter information and influence operations. To achieve the necessary level of integration required to be effective with current authorities and resources I believe we need to become more efficient with the processes that are currently in place with tri-lateral agreements, liaison officers, and other approval processes. If confirmed, I will assess the efficacy of a broader role for USCYBERCOM in this mission space.

Do you agree that it is critical for you, if confirmed, to work on this problem?

Yes.

Use of National Mission Teams to Disrupt Russian Influence Operations

The mission of the National Mission Teams (NMTs) commanded by U.S. Cyber Command is to defend the United States against significant cyber attacks. The NMTs' role is to identify and surveil potential adversary cyber forces, learn as much as possible about those forces and their networks, plans, capabilities, and tactics, and be prepared to disrupt their activities if or when so ordered. The Director of National Intelligence (DNI), in testimony before the Senate Intelligence Committee in February 2018, stated that adversaries, like Russia, will continue to conduct cyber operations to achieve "strategic objectives" even though specific actions are generally perceived to remain below the level of armed aggression or an act of war. The DNI added that adversaries will continue to conduct such operations "unless they face clear repercussions."

Do you agree with the DNI that such operations are intended to and can achieve "strategic effects"? If cyber operations achieve strategic effects, are they by definition of "significant consequence"?

I agree that cyber operations can achieve strategic effects even though they are generally perceived to remain below the threshold of an armed aggression or an act of war. Whether a cyber operation is of significant consequence is assessed on a case-by-case basis.

Do you agree that Russian operations to influence the political views and perceptions of U.S. citizens through social media, traditional media, and the theft and release through cyber means of confidential information owned by candidates and political parties, and the probing of state election systems and databases through cyberspace, constitute significant cyber attacks on the United States?

I concur with the findings of the 2017 Intelligence Community's assessment that Russia clearly conducted a sophisticated campaign to influence the U.S. population that integrated several tools including malicious cyber activities and information operations. I agree with the Director of National Intelligence's recent statement in open testimony that Russia's actions were part of an effort to achieve strategic objectives through low cost deniable means.

Do you agree with expert testimony recently provided to the Senate Armed Services Committee that directing the NMTs to disrupt the ongoing Russian influence operations would be a logical and appropriate use of these forces?

This is an important question and, if confirmed, one that I would be better poised to answer with some time and experience as Commander, USCYBERCOM.

Is there any other element within the U.S. government, aside from intelligence agencies acting under the President's covert action authority, that has the capability and the role to disrupt foreign nation-state cyber attacks on the United States?

The Department of Defense has both the capability and the role to disrupt nation-state cyber attacks on the U.S. by conducting operations to identify, understand, and counter adversary cyber actors and activities outside the U.S. The Department can also provide warning and enabling support to other government agencies that also seek to disrupt cyber attacks. This could include law enforcement actions undertaken by the FBI, protective actions enabled by the Department of Homeland Security in conjunction with sector-specific lead agencies, economic sanctions through the Treasury Department, and diplomatic activities of the State Department.

Should Russian cyber operators be allowed to conduct operations to shape the U.S. democratic political process without disruption?

No.

Has the Secretary of Defense directed U.S. Cyber Command and its component commands to prepare Cyber Mission Forces to disrupt Russian influence operations? Would you recommend such an action to the Secretary if confirmed?

This response would best be answered in a classified setting.

Strategic Effects of Actions Below the Threshold of Armed Aggression

As noted above, the DNI, in testimony before the Senate Intelligence Committee in February 2018, stated that adversaries, like Russia, will continue to conduct cyber operations to achieve "strategic objectives," even though specific actions are generally perceived to remain below the level of armed aggression or an act of war. The Department of Defense's cyber strategy states that Cyber Mission Forces have the mission of defending the United States against cyber attacks of significant consequence. The strategy indicates that attacks of "significant consequences" "may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States."

Does a cyber attack on the United States have to be judged as an armed attack or an armed aggression to qualify as an attack of "significant consequence"?

As noted in the 2015 DoD Cyber Strategy, malicious cyber operations that meet the definition of significant consequences would likely also cross the threshold of an unlawful use of force. However, this requires a case-by-case determination. Although cyber operations not involving loss of life or significant destruction of property may not constitute an armed attack, those operations causing significant impact on U.S. foreign and economic policy interests may nonetheless violate international law and trigger U.S. response options.

Loss of Potent Cyber Tools

Press reports indicate that the CIA suffered a very serious theft of many of its most potent and highly classified cyber intrusion tools. Microsoft Corporation reportedly also suffered from the theft of its database of corporate vulnerabilities. The NSA, according to many reports, has also suffered the loss of a large number of its most powerful cyber tools. Many of these stolen tools have been made public, and many more may be exposed in the future. These tools are in the process of being "weaponized" and used to attack U.S. and allied cyber systems and networks. These weaponized tools are likely to be used against all manner of targets—unconfined to the military or critical infrastructure sector and extending over all types and sizes of companies to steal money or intellectual property.

Do you believe that the U.S. public and our allies have been adequately warned and informed by the U.S. Government of the danger posed by these stolen tools?

Given my current assignment, I am unable to comment on the accuracy of these reported thefts, but if confirmed I will look into the matter.

Has the U.S. Government done all it can to encourage and assist the private sector and allies to remedy the vulnerabilities to these tools?

Given my current assignment, I am unable to comment on the accuracy of these reported thefts, but if confirmed I will look into the matter.

In light of how broad the impact can be of the loss of control of sophisticated cyber exploits on U.S. businesses, do you believe that the Vulnerabilities Equities Process should be altered to include consideration of impacts and risks on society as a whole?

I believe the recent revamping of the Vulnerabilities Equities Process by the White House strikes the right balance between the public's interest in cybersecurity and the protection of critical infrastructure, and the public's interest in effective law enforcement and strong national security.

Organization of the Interagency for Cyber Warfare

The cohesive working and integration of intelligence, homeland defense, law enforcement, and the military are universally recognized as essential to effective cyber defense and deterrence. Cyber operations do not respect organizational boundaries or the distinctions between title 10, title 50, title 18, and title 6. Poor connections, latencies, and doubts about authorities in boundary conditions may prove to be crippling in a serious and fast-moving cyber attack. Great Britain and Israel are examples of two very advanced cyber states that have acted on this reality by establishing organizations at the operational level that merge the capabilities and authorities of multiple government components.

How do you assess the benefits and drawbacks of establishing some sort of interagency organization or task force that integrates capabilities, roles and missions, and authorities to respond to cyber threats?

In my current assignment, I have had limited exposure to the possibility of an interagency organization that might respond to cyber threats. If confirmed, this is an area I would study to become more familiar with the benefits and drawbacks prior to making an assessment.

Constant Contact or Persistent Engagement

Dr. Richard Harknett, the first scholar in residence at U.S. Cyber Command and the NSA, developed a concept for operating in cyberspace that he calls "constant contact," "persistent engagement," and other similar formulations.

How do you interpret the concept of persistent engagement?

Persistent engagement seeks to achieve and maintain the initiative in cyberspace over an adversary by continuously contesting them where they operate, particularly below the level of armed conflict.

Do you believe that Cyber Mission Forces should execute the concept?

This presents an interesting possibility. If confirmed, this is a concept I will study and gain first-hand experience before making an assessment.

Impact of Artificial Intelligence/Machine Learning

Advances in Artificial Intelligence and Machine Learning (AI/ML) driven by the availability of massive data sets on which to learn, and powerful computing platforms to enable rapid learning, promise to enable the automation of sophisticated analysis and adept control of large numbers of complex machines and operations. In the cyber domain, AI/ML may enable cyber forces to achieve much greater levels of scale, speed and intensity. A nation that achieves distinct advantages in these respects may achieve a level of dominance. In contrast, intelligence collection operations in cyberspace the world over are generally characterized as slow, methodical, and manually intensive. U.S. Cyber Command was constructed on top of the capabilities, practices, infrastructure, and training of the NSA.

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

Cyber operators, including our adversaries, increasingly use varying aspects of AI/ML to conduct cyber operations for both offensive and defensive purposes. Within the next three to five years, AI/ML will be commonplace and DoD has begun preparing for it now.

Are U.S. Cyber Command and the military services investing in AI/ML technology at necessary levels, and is there an awareness and acceptance of the significance of this technology for offensive and defensive cyber warfare, and information warfare more broadly?

USCYBERCOM and the military services are investing in AI/ML at a level that is appropriate for their requirements. USCYBERCOM continues to collaborate across the science and technology community to ensure their investments are nested effectively. There is broad awareness and acceptance within DoD/USCYBERCOM of the transformative impact of AI/ML to cyberspace operations. AI/ML technologies offer a great road map for enabling analytic tasks and decision making.

Department of Defense and Department of Homeland Security (DHS)

General Keith Alexander mentioned in his prepared remarks for a May 2017 hearing of the Senate Armed Services Committee that "the perception in industry is that DHS faces significant challenges … in particular that it simply lacks the technical capabilities necessary to succeed."

Do you agree with General Alexander's observation?

If confirmed, I would look to gain more information before agreeing with this observation.

Does DHS have the capability and capacity to defend the United States from a cyber attack by a sophisticated adversary targeting critical infrastructure within the United States?

No single agency can or should be expected to defend the U.S. in isolation; rather, it is essential that we build and refine the processes to share adversary threat data; engage with sector-specific agency partners; build greater resiliency within our critical infrastructure; and leverage a whole-of-nation approach to deter malicious cyber activities.

Does DHS have the capability and capacity to collect intelligence or track threats targeting the United States either domestically or abroad?

If confirmed, I would look to gain more information before making an assessment.

Is the Department of Defense equipped, willing, and able to cover DHS's shortfalls, if called in?

DHS' National Cyber Incident Response Plan outlines domestic cyber incident response coordination and execution among federal, state and territorial, and local governments, and the private sector. DoD partners regularly with DHS on a number of activities. When requested by DHS and directed by the President or Secretary of Defense, DoD will support the response 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.

Do you believe that the Department of Defense's capabilities should be more aggressively utilized by DHS?

I believe recent discussions in response to adversary intrusions in critical infrastructure have led to improved DHS understanding of DoD capacity, capabilities, and the potential for assistance through the Defense Support of Civil Authorities process and believe that DHS will call upon the Department when needed.

Traditional Military Activities

Persistent operations in so-called "red space" are critical for the development of military targets. Without the ability to identify, surveil, and pre-position tools on targets in peacetime, the Department of Defense's ability to provide options to military planners and the President in wartime will be limited. It is the Committee's understanding that the law governing the conduct of clandestine activities in cyberspace may need to be clarified to overcome objections within the interagency to U.S. Cyber Command operations outside areas of declared hostilities. Elements of the Intelligence Community and other executive branch departments and agencies have often argued within the interagency that some Department of Defense activities outside a designated area of hostilities should be constrained because clandestine cyberspace operations may not qualify as a Traditional Military Activity under the current legal framework.

Do you agree or disagree with the argument that clandestine offensive cyber operations conducted outside a declared area of hostilities are inherently covert actions and not Traditional Military Activities?

Clandestine cyber operations outside a declared area of hostilities are not inherently covert action, as that term is used in U.S. law, and could be conducted as traditional military activities. "Traditional military activity" is not statutorily defined but informed by legislative history and past Executive Branch practice. Whether a military operation is a traditional military activity is a fact specific determination made on a case-by-case basis. .

How does such an interpretation of Traditional Military Activity impact U.S. Cyber Command's ability to develop military cyber options for the President?

Based on the evolving nature of adversary cyber capabilities and threats, UCYBERCOM must be postured to defend the Nation in and through cyberspace, which may necessitate conducting certain cyber activities and operations outside of armed conflict or declared areas of hostilities. These activities or operations can be conducted when consistent with the provisions of the traditional military activity exception to the definition of covert action. Those activities or operations that constitute traditional military activities afford the Commander, USCYBERCOM, an additional degree of flexibility in developing and executing cyber options for or on behalf of the President.

Assuming the concern is about operational preparation of the environment in cyberspace, is it realistic to expect our forces to be able to provide capability with any degree of certainty against a proficient adversary if they are unable to establish digital footholds in advance of hostilities?

To be operationally effective in cyberspace, U.S. forces must have the ability to conduct a range of preparatory activities which may include gaining clandestine access to operationally relevant cyber systems or networks.

Do you believe the latitude for operational preparation of the environment conducted under title 10 authorities today is sufficient to meet the current and projected operational requirements of the Cyber Mission Force?

At present, USCYBERCOM has the authority to conduct a range of enabling activities necessary to be prepared to conduct operations, and when directed, to defend the Nation. If confirmed, I will pursue the additional operational authorities I believe necessary based on threat evaluation and mission requirements.

How do issues concerning intelligence gain/loss and operational gain/loss influence your views concerning operational preparation of the environment under the existing dual hat arrangement? How might that change in a non-dual hat scenario?

It is always important when conducting any military operation to consider the equities of potentially affected departments and agencies. In a “dual-hat” arrangement, the Commander, USCYBERCOM/Director of the NSA has the ability to weigh USCYBERCOM’s operational mission against the intelligence equities of the NSA and reach a best-fit decision. In a non-“dual-hat” scenario, that decision making authority will reside at a higher level of command.

Do you support clarifying what qualifies as a Traditional Military Activity in cyberspace?

Providing greater clarity on what constitutes traditional military activities could facilitate more effective planning and execution of military cyberspace operations.

Department of Defense Information Networks

Do you believe that the Department of Defense’s defense of its information networks is robust?

Yes. The Department has a robust, defense in depth approach that employs multiple capabilities at different levels in our networks and enables our defenders to generate tailored effects and mitigation strategies. Notably, the employment of DoD's nine certified cyber red teams in a "persistent cyber opposing force (OPFOR)" role, as well as the growing use of innovative "Bug Bounty" programs in the Department, leads to the continuous testing and strengthening of our information networks’ defense.

How can the Department’s cybersecurity be improved?

The Department’s defenses must continue to keep pace with the growing and evolving capabilities of cyber threat actors. DoD cybersecurity could be further improved by adherence to and enforcement of all cybersecurity protocols including ensuring strong authentication; hardening devices; reducing the attack surface; and improved detection of and response to potential intrusions. In recent years, the Department’s approach to cyber defense has been shifting from one striving to be a "fast follower" of industry cybersecurity best-of-breed cybersecurity capabilities, toward a threat-based analysis that evaluates DoD's cyber defenses against the most capable cyber actors, and seeks new defensive elements and upgrades to address new vulnerabilities.

How is the Department planning to address the Spectre and Meltdown hardware vulnerabilities?

USCYBERCOM is engaged with the intelligence community, interagency, and industry to better understand Spectre and Meltdown vulnerabilities and employ mitigations. JFHQ-DoDIN has issued an order incorporating the initial set of Information Assurance Vulnerability Management (IAVM) directives addressing the these vulnerabilities. Additional IAVM releases, issued in concert with recommendations by USCYBERCOM for prioritization, will continue on a regular basis as vendors and chip makers provide fixes. Given the performance degradation in the fixes industry has provided chip vulnerabilities to date, coupled with a lack of effective exploits observed in the wild (beyond basic "proof of concept" code from security researchers), the Department will need to continue to follow these developments closely and adjust its approach as the situation warrants.

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

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. Using the guidelines in DODI 1100.22, they identify which functions are inherently governmental, then determine which will be performed by DoD civilians, and which will or must be performed by military personnel.

What are the legal and policy parameters surrounding the use of contractor personnel?

Contractors are an integral part of the team and fulfill a variety of important functions for USCYBERCOM. These functions encompass vital support to both the Command, and the CMF engaged in operations. We must also maintain sufficient “in-house” expertise for these critical functions, however, to adequately oversee and manage the contractor workforce. It is essential that military personnel and government civilians maintain proper oversight and ensure inherently government functions are performed by government personnel.

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?

I believe that USCYBERCOM is on track for the appropriate force mix at this time given the present hiring environment. USCYBERCOM has received additional allocations under the Joint Chiefs of Staff Cyber Command and Control order, and these will take the Command to a mix of approximately 80 percent military members and 20 percent civilian personnel and contractors.

From what I have been told, this mix is about right given the educational, legal, and recruiting constraints the Command faces.

Congressional Oversight

In order to exercise its legislative and oversight responsibilities, it is important that this Committee and other appropriate committees of Congress are able to receive testimony, briefings, and other communications of information.

Do you agree, if confirmed, to appear before this Committee and other appropriate committees of Congress?

Yes.

Do you agree, if confirmed, to appear before this Committee, or designated members of this Committee, and provide information, subject to appropriate and necessary security protection, with respect to your responsibilities as Commander of U.S. Cyber Command and Director of the National Security Agency/Chief of the Central Security Service?

Yes.

Do you agree to ensure that testimony, briefings, and other communications of information are provided to this Committee and its staff and other appropriate committees in a timely manner?

Yes.

Do you agree to provide documents, including copies of electronic forms of communication, in a timely manner when requested by a duly constituted committee, or to consult with this Committee regarding the basis for any good faith delay or denial in providing such documents?

Yes.

Do you agree to answer letters and requests for information from individual Senators who are members of this Committee?

Yes.

If confirmed again, do you agree to provide to this Committee relevant information within the jurisdictional oversight of the Committee when requested by the Committee, even in the absence of the formality of a letter from the Chairman?

Yes.