Advance Questions for Lieutenant General Keith Alexander, USA
Nominee for Commander, United States Cyber Command

1. Defense Reforms

The Goldwater-Nichols Department of Defense Reorganization Act of 1986 and the Special Operations reforms have strengthened the warfighting readiness of our Armed Forces. They have enhanced civilian control and clearly delineated the operational chain of command and the responsibilities and authorities of the combatant commanders, and the role of the Chairman of the Joint Chiefs of Staff. They have also clarified the responsibility of the Military Departments to recruit, organize, train, equip, and maintain forces for assignment to the combatant commanders.

1a) Do you see the need for modifications of any Goldwater-Nichols Act provisions?

(U) The integration of joint capabilities under the Goldwater-Nichols Act has been a remarkable achievement. Our military forces are more interoperable today than they ever have been in our nation's history. I do not see a need to modify the Goldwater-Nichols Act at this time.

1b) If so, what areas do you believe might be appropriate to address in these modifications?

2. Duties

2a) What is your understanding of the duties and functions of the Commander, U. S. Cyber Command?

(U) In accordance with SECDEF guidance of June 23, 2009, the Commander, U.S. Cyber Command is responsible for executing the specified cyberspace missions detailed in Section 18.d.(3) of the Unified Command Plan (UCP) as delegated by the Commander, U.S. Strategic Command to secure our freedom of action in cyber space and mitigate the risks to our national security that come from our dependence on cyberspace and the associated threats and vulnerabilities. Subject to the Commander, U.S. Strategic Command delegation and in coordination with mission partners, specific missions include: integrating cyberspace operations and synchronizing warfighting effects across the global security environment; providing support to civil authorities and international partners; directing global information grid operations and defense; executing full-spectrum military cyberspace operations; serving as the focal point for deconfliction of DOD offensive cyberspace operations; providing improved shared situational awareness of cyberspace operations, including indications and warning; and providing military representation to U.S. national agencies, U.S. commercial agencies, and international agencies for cyberspace matters.

2b) What background and experience do you possess that you believe qualifies you to perform these duties?

(U) I am deeply honored that the President nominated me to be the first Commander of U.S. Cyber Command. Over the past three decades, I have served in a wide variety of Joint and Army positions, including 15 years in command, that have prepared me well for the challenges ahead if confirmed by the U.S. Senate.

(U) First, I have 35 years in the profession of arms, serving in various command, staff and intelligence positions in the military. I have served as the Deputy Chief of Staff of Intelligence, Headquarters, Department of the Army; Commanding General of the US Army Intelligence and Security Command; Director of Intelligence, United States Central Command; and Deputy Director for Requirements, Capabilities, Assessments and Doctrine, J-2, for the Joint Chiefs of Staff.

(U) Second, my experiences and knowledge gained over the last four and a half years serving as Director, National Security Agency, Chief, Central Security Service and Commander, Joint Functional Component Command-Network Warfare (JFCC-NW) have been instrumental in preparing me for the challenges of this new complex warfighting domain that is cyberspace. NSA's cryptologic work in SIGINT/Computer Network Exploitation, Information Assurance and Network Threat Operations is second to none and foundational to our future success in the cyber domain. I have personally championed NSA's work and learned a great deal from the outstanding professionals at NSA/CSS. Over the last four and a half years, I have also forged important partnerships with both our allies and with industry to strengthen the defense of our collective networks. Furthermore, my assignment as the Commander, JFCC-NW, including operational control over Joint Task Force-Global Network Operations (JTF-GNO) for the past 18 months, has provided me with the experience, particularly in the realm of deliberate and crisis action planning, to ensure the effective execution of cyberspace responsibilities as directed by the SECDEF through Commander, U.S. Strategic Command.

(U) Finally, I believe my academic background has intellectually prepared me for the challenges of high-level command and complex environments. I have Masters of Science degrees in Business Administration, Systems Technology (Electronic Warfare) and Physics, as well as National Security Strategy.

2c) If confirmed as the Commander of U.S. Cyber Command, would you have command of or exercise operational control of the Defense Information Systems Agency's and military services' communications networks?

(U) If confirmed as Commander, U.S. Cyber Command, I will be responsible for directing the operation and defense of DOD's military information networks as specified in the Unified Command Plan (UCP) and as delegated by Commander, U.S. Strategic Command. I will execute this mission through each of the Service Network Operations and Security Centers (NOSC). I will not exercise command or operational control over the Defense Information Systems Agency communications networks. DISA will continue

to be responsible for acquiring, engineering and provisioning enterprise infrastructure to assure the availability of military information networks. As a Combat Support Agency, DISA will maintain a close working relationship with U.S. Cyber Command, providing expertise on the networks, communications and computing infrastructure operated by DISA through both a DISA Field Office and a DISA Support Element.

2d) As a career intelligence officer, what experience do you have that qualifies you to command these networks and to command military forces and military operations?

(U) Answer provided in the classified supplement.

2e) 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?

(U) I fundamentally believe that there is always something to be learned to enhance my expertise in this very complex and dynamically changing domain. If confirmed, I will engage with Combatant Commanders to understand better how U.S. Cyber Command can best support and help meet their operational missions. Additionally, I would engage with key officials and personnel within the Executive and Legislative branches of the United States government, senior military leaders, and leaders throughout the Intelligence Community in order to identify, assess, and mitigate the cyber threats we face.

2f) Is there a precedent for a career intelligence officer to serve as a Combatant Commander?

(U) I know of no career intelligence officers who have previously served as either a Combatant or Sub-Unified Commander. However, two former Directors of the National Security Agency, General Lew Allen and Admiral Noel Gayler, served with great distinction as the Chief of Staff, US Air Force and Commander, U.S. Pacific Command, respectively.

3. <u>Relationships</u>

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 the Commander, U. S. Cyber Command, will have to the following officials:

3a) The Secretary of Defense

(U) Pursuant to title 10, U.S.C., section 164, subject to the direction of the President, the Commander, U.S. Strategic Command, 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 missions assigned to the command. As a sub-unified command under the authority, direction, and control of the Commander, U.S. Strategic Command, U.S. Cyber Command will be directly responsible to the Secretary of Defense through the Commander, U.S. Strategic Command . If confirmed, I will work closely with the Secretary in coordination with Commander, U.S. Strategic Command, on matters of strategic importance.

3b) The Deputy Secretary of Defense

(U) In accordance with title 10, U.S.C., section 132, the Deputy Secretary of Defense will perform such duties and exercise 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, in coordination with Commander, U.S. Strategic Command, on matters of strategic importance.

3c) The Director of National Intelligence

(U) The Intelligence Reform and Terrorist Prevention Act of 2004 established the Director of National Intelligence to act as the head of the Intelligence Community, principal advisor to the President, National Security Council, and Homeland 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 is responsible to coordinate national intelligence priorities and to facilitate information sharing among the Intelligence Community. If confirmed, I will work closely with the Commander, U.S. Strategic Command and through the Secretary of Defense to coordinate and exchange information with the Director of National Intelligence as needed to ensure unified effort and the leveraging of available synergies within the Intelligence Community to support matters of national security.

3e) The Under Secretary of Defense for Policy

(U) Title 10, U.S.C. and current DOD directives establish the Under Secretaries of Defense as the principal staff assistants and advisors to the Secretary of Defense regarding matters related to their respective functional areas. Within these areas, the Under Secretaries exercise policy and oversight functions, and in discharging their responsibilities, the Under Secretaries may issue instructions and directive memoranda that implement policy approved by the Secretary. If confirmed, I look forward to working with the Under Secretary of Defense for Policy, in coordination with Commander, U.S. Strategic Command, on all policy issues that affect U.S. Cyber Command operations.

3f) The Under Secretary of Defense for Intelligence

(U) Title 10, U.S.C. and current DOD directives establish the Under Secretaries of Defense as the principal staff assistants and advisors to the Secretary of Defense regarding matters related to their respective functional areas. Within these areas, the Under Secretaries exercise policy and oversight functions and, in discharging their responsibilities the Under Secretaries may issue instructions and directive memoranda that implement policy approved by the Secretary. If confirmed, I look forward to working with the Under Secretary of Defense for Intelligence, in coordination with Commander, U.S. Strategic Command, on matters in the area of U.S. Cyber Command's assigned responsibilities.

3g) The Under Secretary of Defense for Acquisition, Technology, and Logistics

(U) Title 10, U.S.C. and current DOD directives establish the Under Secretaries of Defense as the principal staff assistants and advisors to the Secretary of Defense regarding matters related to their respective functional areas. Within these areas, the Under Secretaries exercise policy and oversight functions and, in discharging their responsibilities the Under Secretaries may issue instructions and directive memoranda that implement policy approved by the Secretary. If confirmed, I look forward to working with the Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with Commander, U.S. Strategic Command, on matters in the area of U.S. Cyber Command's assigned responsibilities.

3h) The Assistant Secretary of Defense for Networks and Information Integration

(U) Under the authority of Department of Defense Directive 5144.1 and consistent with Titles 10, 40, and 44, U.S.C., the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) serves as the DOD Chief Information Officer (CIO) and is the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on networks and network-centric policies and concepts; command and control (C2); communications; non-intelligence space matters; enterprise-wide integration of DOD information matters; Information Technology (IT), including National Security Systems (NSS); information resource management (IRM); spectrum management; network operations; information systems; information assurance (IA); positioning, navigation, and timing (PNT) policy, including airspace and military-air-traffic control activities; sensitive information integration; contingency support and migration planning; and related matters. Pursuant to chapter 113, subchapter III of 40 U.S.C., the ASD(NII)/DOD CIO has responsibilities for integrating information and related activities and services across the DOD. If confirmed, I look forward to working with the Assistant Secretary of Defense for Networks and Information Integration through the Secretary and Deputy Secretary of Defense and Commander U.S. Strategic Command on matters in the area of U.S. Cyber Command's assigned responsibilities.

3i) The Assistant Secretary of Defense for Homeland Defense

(U) The Assistant Secretary of Defense for Homeland Defense executes responsibilities including overall supervision of the homeland defense activities of the DOD while

serving under the Under Secretary of Defense for Policy. Any relationship the Commander, U.S. Cyber Command requires with the Assistant Secretary of Defense for Homeland Security would exist with and through the Under Secretary of Defense for Policy. If confirmed, I look forward to working with the Assistant Secretary of Defense for Homeland Defense in concert with Commander, U. S. Strategic Command, Commander, U.S. Northern Command, and Commander, U.S. Pacific Command on related national security issues.

3j) The Chairman of the Joint Chiefs of Staff

(U) The Chairman is the principal military advisor to the President, National Security Council, and Secretary of Defense. Title 10, United States Code, 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, I would normally communicate with the Chairman in coordination with the Commander, U.S. Strategic Command.

3k) The Secretaries of the Military Departments

(U) Under 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 quite clear but requires close coordination with each Secretary to ensure that 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 Commander, U.S. Strategic Command.

3m) The Chiefs of Staff of the Services

(U) 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 will work closely and confer regularly with the Service Chiefs.

3n) The Combatant Commanders and specifically the Commanders of U.S. Strategic Command and U. S. Northern Command

(U) U.S. Cyber Command is a subordinate unified command under U.S. Strategic Command. The Commander, U.S. Cyber Command will have 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, U.S. Cyber Command will be 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 Commander, U.S. Northern Command will be delineated by the SECDEF or the President in execute and/or operation orders. If confirmed, I look forward to working with the combatant commanders to broaden and enhance the level and range of these relationships.

3p) The Director of the Defense Information Systems Agency

(U) The Defense Information Systems Agency (DISA) is a DOD combat support agency that provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to join war fighters, National-level leaders, and other mission and coalition partners across the full spectrum of operations. Commander, U.S. Cyber Command must maintain a close relationship with the Director, DISA to coordinate and represent requirements in this mission area, in order to accomplish U.S. Strategic Command delegated UCP missions. To this end, LTG Pollett, the current Director of DISA, has committed to providing both a DISA Field Office (DFO) as well as a DISA support element (DSE) unique to U.S. Cyber Command. If confirmed, I will continue to work closely with the Director of DISA on matters of shared interest and importance.

4. <u>Oversight</u>

The duties of the Commander, U.S. Cyber Command will include conducting integrated intelligence collection and offensive and defensive operations in cyberspace. However, the resourcing, planning, programming and budgeting, and oversight of these three basic activities is fragmented within the Department of Defense (DOD), the executive branch as a whole, and within Congress. Multiple elements within the Office of the Secretary of Defense and the Joint Staff have responsibilities for one or more of the missions of Cyber Command. The same is true for the Secretary of Defense and the Director of National Intelligence, as well as the Armed Services and Intelligence Committees in Congress. The single point of confluence would be the Commander of Cyber Command, dual-hatted as the Director of the National Security Agency (NSA).

4a) How do you anticipate that the Department will ensure the necessary degree of coordination and timely decision-making across the Department to guide the operations and resourcing of Cyber Command?

(U) Through the Secretary of Defense's policy initiatives for cyberspace operations and implementation guidance concerning national security directives, the Department will ensure the necessary degree of coordination and timely decision-making across the Department to guide the operations and resourcing of U.S. Cyber Command. If confirmed, I envision that the Department will retain its commitment to close

coordination both internally and externally to guide the operations and resourcing of this command.

4b) What is the risk, in your view, that this fragmented policy and oversight structure will result in a lack of coherent oversight of cyberspace and U.S. Cyber Command?

(U) I believe we have a coherent policy and oversight structure in place for cyberspace and that there is no risk that we will lack coherent oversight. If confirmed, I can assure you that my actions will be guided by the authorities vested in me by the SECDEF and Commander, U.S. Strategic Command and oversight of my actions will be clearly auditable for overseers.

5. Major Challenges and Problems

5a) In your view, what are the major challenges that will confront the Commander, U.S. Cyber Command?

(U) I believe the major challenge that will confront the Commander, U.S. Cyber Command will be improving the defense of our military networks as they exist today. Additionally, in order to defend those networks and make good decisions in exercising operational control over them, U.S. Cyber Command will require much greater situational awareness and real-time visibility of intrusions into our networks. Finally, I believe the Commander, U.S. Cyber Command will have to identify continuously policy and authority gaps to U.S. Strategic Command and our civilian leadership as computer and communication technologies evolve.

5b) Assuming you are confirmed, what plans do you have for addressing these challenges?

(U) Answer provided in the classified supplement.

5c) What are your priorities for the U.S. Cyber Command?

(U) Answer provided in the classified supplement.

6. U. S. Cyber Command Missions

6a) In an overarching sense, how do you define the U.S. Cyber Command missions?

(U) Answer provided in the classified supplement.

7. Offensive Cyber Warfare Capabilities

The attached solicitations and program descriptions show that the military services are developing capabilities to stealthily penetrate foreign computer networks, maintain a presence on those networks, collect and extract information clandestinely, and undertake offensive actions. The National Military Strategy for Cyberspace Operations, published in 2006, also indicates that the U.S. military places considerable importance on acquiring potent offensive cyber warfare capabilities.

7a) Does DOD possess significant capabilities to conduct military operations in cyberspace at the tactical, operational, and strategic levels?

(U) Answer provided in the classified supplement.

7b) Is there a substantial mismatch between the ability of the United States to conduct operations in cyberspace and the level of development of policies governing such operations?

(U) President Obama's cybersecurity sixty-day study highlighted the mismatch between our technical capabilities to conduct operations and the governing laws and policies, and our civilian leadership is working hard to resolve the mismatch. In the June 23, 2009 memorandum outlining the establishment of U.S. Cyber Command, the Secretary of Defense directed the Under Secretary of Defense for Policy to lead a review of policy and strategy to develop a comprehensive approach to DOD cyberspace operations. This review is active and ongoing.

7c) Are you concerned that you are being assigned to command an organization that may be directed to conduct activities whose legality and rules have not been worked out?

(U) Given current operations, there are sufficient law, policy, and authorities to govern DOD cyberspace operations. If confirmed, I will operate within applicable laws, policies, and authorities. I will also identify any gaps in doctrine, policy and law that may prevent national objectives from being fully realized or executed to the Commander, U.S. Strategic Command and the Secretary of Defense.

7d) When does the administration intend to close existing policy gaps?

(U) The administration has provided a comprehensive set of cyber security initiatives that will inform policy making (e.g., Comprehensive National Cybersecurity Initiative (CNCI) and the President's Strategy to Secure Cyberspace). In support of the Secretary of Defense, we will continue to work to identify gaps, inform the development of

meaningful and enduring national cyber policy, and be prepared to adjust rapidly to changes.

8. Support to the Comprehensive National Cybersecurity Initiative

Under the Comprehensive National Cybersecurity Initiative (CNCI), the National Security Agency is providing support to the Department of Homeland Security.

8a) What is the nature and extent of that support?

(U) Answer provided in the classified supplement.

8b) Is this support provided as a DOD activity or as an intelligence activity through the Director of National Intelligence? If the latter, what is the Secretary of Defense's role as the President's executive agent for signals intelligence under Executive Order 12333?

(U) The support provided by NSA to DHS is provided as a DOD activity, in coordination with the Director of National Intelligence.

(U) Specifically, with respect to the Foreign Intelligence support to DHS, per Executive Order 12333, as amended, NSA is an element of both the Intelligence Community, of which the Director of National Intelligence serves as the head, and the Department of Defense, whose Secretary acts, in coordination with the Director of National Intelligence, as the Executive Agent for the United States Government for signals intelligence activities. In these capacities, NSA conducts signals intelligence activities for both national and departmental requirements.

(U) Further, with respect to Information Assurance support to DHS, for such support that is given in connection with national security systems, National Security Directive 42 provides that the Secretary of Defense shall serve as the Executive Agent of the Government for National Security Telecommunications and Information Systems Security. NSD 42 further designates the Director NSA as the National Manager for National Security Telecommunications and Information's Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out those responsibilities. With respect to Information Assurance support to DHS that is provided in connection with non-national security systems, NSA is authorized by EO12333 to provide technical assistance to other United States Government departments and agencies for either national security systems or non-national security systems.

9. Support to Civil Authorities

DOD officials have informed the Committee that U.S. Cyber Command will have a mission to support civil authorities, such as the Department of Homeland Security and law enforcement agencies, to help defend government networks and critical infrastructure networks owned and operated by the private sector.

9a) Please describe in detail your understanding of the ways that U.S. Cyber Command is most likely to assist civil authorities.

(U) If I am confirmed as Commander, U.S. Cyber Command, I will work closely with the Commanders of U.S. Strategic Command and U.S. Northern Command to answer any Request For Assistance (RFA) from the Department of Homeland Security. Our assistance could include technical assistance and recommendations for immediate defensive actions, as well as technical assistance and recommendations for more systemic mitigation, such as improvements in network configurations and improvements in information assurance measures or best practices. Additionally, U.S. Cyber Command would continually assess the cyber threat to DOD's information systems to ensure we are prepared to provide cyber support to civil authorities in the event of a cyber threat to the Nation's critical infrastructure.

U.S. Northern Command was established to serve as the focal point for DOD support to civil authorities.

9b) Will cybersecurity support to civil authorities be provided through U.S. Northern Command, as a supported command, or otherwise? If not, why not?

(U) Answer provided in the classified supplement.

10. <u>Use of Force in Cyberspace</u>

10a) Does DOD have a definition for what constitutes use of force in cyberspace, and will that definition be the same for U.S. activities in cyberspace and those of other nations?

(U) Article 2(4) of the UN Charter provides that states shall refrain from the threat or use of force against the territorial integrity or political independence of any state. DOD operations are conducted consistent with international law principles in regard to what is a threat or use of force in terms of hostile intent and hostile act, as reflected in the Standing Rules of Engagement/Standing Rules for the Use of Force (SROE/SRUF).

(U) There is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force. Thus, whether in the cyber or any other domain, there is always potential disagreement among nations concerning what may amount to a threat or use of force.

(U) Remainder of answer provided in the classified supplement.

10b) Has DOD or the administration as a whole determined what constitutes use of force in cyberspace in relation to the War Powers Act, the exercise of the right of self-defense under the UN Charter, and the triggering of collective defense obligations? If not, when will these fundamental policy issues be resolved?

(U) The President of the United States determines what is a threat or use of force/armed attack against the United States and authorizes DOD through the SROE to exercise our national right of self-defense recognized by the UN Charter. This determination involves an objective and subjective analysis that considers the facts surrounding a particular cyber attack, and is made within the bounds of U.S. and international law. If the President determines a cyber event does meet the threshold of a use of force/armed attack, he may determine that the activity is of such scope, duration, or intensity that it warrants exercising our right to self-defense and/or the initiation of hostilities as an appropriate response. It is also within the President's authority to determine, based upon the circumstances of any event, including a cyber event, and the contemplated response, what consultations and reports to Congress are necessary consistent with the provisions of the War Powers Resolution. The UN Charter recognizes a state's inherent right of individual and collective self-defense, and the United States would evaluate its collective defense obligations when another state is threatened or subject to a use of force in the cyber domain just as it would in the other warfighting domains.

10c) Could U.S. Cyber Command lawfully employ offensive cyber weapons against computers located abroad that have been determined to be sources of an attack on the United States or U.S. deployed forces if we do not know who is responsible for the attack (i.e., a foreign government or non-state actors)?

(U) The establishment of U.S. Cyber Command, in and of itself, does not change the lawful employment of military force for self-defense. In this case, if the "attack" met the criteria approved by the President in our Standing Rules of Engagement, the military would exercise its obligation of self-defense. Operationally, it is difficult to develop an effective response when we do not know who is responsible for an "attack"; however, the circumstances may be such that at least some level of mitigating action can be taken even when we are not certain who is responsible. Regardless whether we know who is responsible, international law requires that our use of force in self-defense be proportional and discriminate. Neither proportionality nor discrimination requires that we know who is responsible before we take defensive action.

10d) Without confident "attribution," under international law, would DOD, in your judgment, be allowed to "fire back" without first asking the host government to deal with the attack?

(U) Answer provided in the classified supplement.

Traditionally, espionage has not been regarded as a use of force or an act of war. Generally speaking, in cyberspace operations, experts agree that gaining access to a target for intelligence collection is tantamount to gaining the ability to attack that target. If a penetration is detected, the victim cannot determine whether the purpose of the activity is limited to espionage or also constitutes preparation for an attack.

10e) With the foregoing in mind, are there or should there be classes of U.S. or allied targets that the U.S. Government would consider off-limits from hostile penetration because of the danger that any such breaches would present to national security?

(U) Answer provided in the classified supplement.

10f) Would or should such targets be immune to penetration by the United States in peacetime even for intelligence collection?

(U) Answer provided in the classified supplement.

11. <u>Authorities of Commander, U.S. Cyber Command</u>

Offensive cyber warfare weapons or operations could have devastating effects, depending on the target of the attack and the method used, which conceivably could be comparable to those caused by weapons of mass destruction.

11a) If confirmed as Commander, U.S. Cyber Command, would you have the authority to use offensive cyber weapons against the following representative classes of targets:

Military command & control networks;
Military air defense networks;
Military platforms and weapons;
Power grids;
Banks and other financial institutions and networks;
Transportation-related networks; and
National telecommunications networks?

(U) The categories listed are all potential targets of military attack, both kinetic and cyber, under the right circumstances. It is difficult for me to conceive of an instance where it would be appropriate to attack a bank or a financial institution, unless perhaps it was being used solely to support enemy military operations.

(U) Offensive cyber weapons would only be authorized under specific lawful orders by the SECDEF and the President and would normally come with supplemental rules of engagement.

(U) All military operations, to include actions taken in cyberspace, must comply with international law that governs military operations. Specifically, any U.S. military

operation must comport with the principles of military necessity, discrimination, and proportionality. These legal principles are addressed during the planning and operational phases of all military operations.

11b) Do you have this authority now as the Joint Functional Component Commander for Network Warfare?

(U) Answer provided in the classified supplement.

11c) At what level of command can decisions be made to pre-deploy offensive cyber weapons against these same classes of targets? Will this change after the standup of U.S. Cyber Command?

(U) This authority rests with SECDEF and the President. It will not change after U.S. Cyber Command is established.

Operations in cyberspace occur at nearly the speed of light. Speed of response is widely considered to be necessary in some circumstances when operating in cyberspace.

11d) Is there currently or do you anticipate that there will be a requirement to pre-authorize the use of force in cyberspace below the level of the National Command Authority? If so, to what level and in what circumstances?

(U) Answer provided in the classified supplement.

11e) Is it your understanding that, as is the case with the Commander of the sub-unified U.S. Forces Korea Command, the sub-unified Commander of Cyber Command will have freedom of action to fight the war?

(U) The Commander of U.S. Cyber Command will have freedom of action to conduct military operations in cyberspace based upon the authorities provided by the President, the Secretary of Defense, and the Commander, U.S. Strategic Command. Because cyberspace is not generally bounded by geography, the Commander of U.S. Cyber Command will have to coordinate with U.S. agencies and Combatant Commanders that would be affected by actions taken in cyberspace.

11f) What is the role of the Commander, U.S. Strategic Command, in directing or approving courses of action of the Commander, U.S. Cyber Command?

(U) Commander, U.S. Strategic Command, as the Combatant Commander, has the responsibility to specify U.S. Cyber Command missions and tasks and delegate appropriate authority to accomplish those tasks. In accordance with joint doctrine, authority is normally given to subordinate commanders to select the methodology for

accomplishing the mission, including selection and approval of courses of action. However, this authority may be limited by directives or other orders of the superior commander. Commander, U.S. Strategic Command has indicated to the Secretary of Defense he will delegate authority for all Unified Command Plan cyber tasks, with the exception of advocacy for cyberspace capabilities and integration of the Theater Security Cooperation activities with Geographic Combatant Commanders.

12. Laws of War

12a) Has DOD determined how the laws of armed conflict (including the principles of military necessity in choosing targets, proportionality with respect to collateral damage and unintended consequences, and distinguishing between combatants and non-combatants) apply to cyber warfare with respect to both nation-states and non-state entities (e.g., terrorists, criminals), and both when the source of an attack is known and unknown?

(U) Per DOD guidance, all military operations must be in compliance with the laws of armed conflict—this includes cyber operations as well. The law of war principles of military necessity, proportionality and distinction will apply when conducting cyber operations.

12b) If not, when will the Department produce authoritative positions on these issues?

13. Balancing Equities

There have been many instances in history where military and political leaders had to struggle with the choice of acting on intelligence information to save lives or forestall an enemy success but at the cost of the enemy learning that their communications, information, or capabilities had been compromised. These choices are referred to as "balancing equities" or "gain-loss" calculations. U.S. Cyber Command is to be headed by the Director of the NSA, which, like all intelligence agencies, could be naturally expected to seek to protect sensitive sources and methods.

13a) Who will be in charge of the equities/gain-loss process for cyberspace within the military?

(U) Within DOD, the equities/gain-loss process is built into the deliberate and crisis action planning process and initiated by the Combatant Commanders. In most cases, the gain-loss recommendation within DOD is initially made by the supported Combatant Commander after the risk of loss is well articulated by the intelligence community. If there is disagreement I, as the commander of JFCC NW, serve as the focal point for DOD offensive cyberspace operations in accordance with the deconfliction process directed in NSPD-38. If the NSPD-38 deconfliction process does not resolve the interagency disagreement, the issue goes to the Chairman, Joint Chiefs of Staff, the Secretary of

Defense, the NSC Deputies, the NSC Principals, and then the President, where the gain-loss determination continues to be considered. (In counter-terrorism issues, the National Counter-Terrorism Center is brought in before the Deputies Committee considers the issue.) If confirmed as Commander of U.S. Cyber Command, I will continue to have responsibility for this process within the Department.

13b) If these decisions will rest with the Commander of Cyber Command, how would you expect the process to work to ensure that the combatant commands, the military services, and other defense agencies have the opportunity to defend their interests and are not overruled by NSA?

(U) We would use the process outlined by the Joint Staff and used by other combatant commands. Intelligence Gain-Loss is a consideration of target vetting and is coordinated with the Intelligence Community agencies and with supporting combatant commands throughout the planning process. Those agencies and commands provide comments on their equities and issues for the commander's review and validation. The supported command then makes a determination based on their mission and expected effects. If the targeting issues cannot be resolved between the Commander, U.S. Cyber Command / Director, NSA and the FBI Cyber Division, the issue goes to the NSC Deputies Committee, and if still unresolved, the NSC Principals Committee.

13c) If confirmed, how will you ensure that equities/gain-loss decisions are made for the nation as a whole? How will the interests of the vulnerable private sector, critical infrastructure, and civil agencies be weighed in the selection of targets for intelligence collection and attack in wartime?

(U) Our deconfliction process, documented in a Tri-lateral Memorandum of Agreement among DOD, DoJ and the Intelligence Community, includes appropriate representation of other agencies as directed in NSPD-38. As with targeting issues within the Department, the reclama process for issues spanning Federal agencies matriculate from the Seniors to the Deputies Committee to the Principals Committee if they remain unresolved.

14. <u>Deterrence and Escalation Control</u>

The U.S. Government currently does not appear to have a cyber warfare deterrence strategy or doctrine. Promulgating such a doctrine requires at least some broad statements of capabilities and intentions regarding the use of offensive cyber capabilities, both to influence potential adversaries and to reassure allies. Such statements are not possible given the current degree of classification of all aspects of US cyber warfare capabilities.

14a) Do you agree that it is necessary to declassify some information about U.S. cyber warfare capabilities in order to support deterrence and engagement with allies and potential adversaries?

(U) I agree and fully support the President's Executive Order regarding security classification. This is a complex subject, and we will continue to implement directed policies and inform policy-makers of operational impacts.

14b) Is there a process and timetable in place to accomplish this objective?

(U) I am not aware of any plan or timetable to declassify detailed information about U.S. offensive cyber capabilities. Articulating new processes and timetables would flow from direction set by the White House.

Most experts believe that the attacker has a substantial advantage over the defender in cyber warfare. It is also widely believed that preemptively striking first against an adversary's networks offers an advantage if the adversary's command and control networks can be degraded, and because the attacker can take steps to protect itself from a retaliatory attack. These considerations suggest that cyber warfare is currently "unstable" from the perspective of classic deterrence theory and escalation control.

14c) Do you, or to your knowledge, experts in the Department, have a different view of these dynamics?

(U) I'd certainly agree that cyber warfare has unique and important differences from classic deterrence theory and escalation control. Experts, both inside and outside government, as well as within the Department of Defense and Intelligence Communities, have widely differing views of these dynamics, as should be expected. A consensus has yet to emerge, either on how to characterize the strategic "instability" or on what to do about it.

15. <u>U.S. Military Strategy in Cyberspace</u>

The National Military Strategy for Cyberspace Operations (NMS-CO), December 2006, states that "The United States must have cyberspace superiority to ensure our freedom of action and deny the same to our adversaries through the integration of network defense, exploitation, and attack…The NMS-CO is the comprehensive military strategy for the U.S. Armed Forces to ensure U.S. superiority in cyberspace."

15a) Is this strategy statement consistent with current policy? If not, is there a plan to issue a new or revised NMS-CO?

(U) Answer provided in the classified supplement.

15b) Is this strategy realistic in light of the vulnerability of U.S. government and private networks to attack?

(U) The military strategic goal of cyberspace superiority is realistic, but not without difficulty in achieving its objectives in the current national security environment. The 42 tasks in the NMS-CO Implementation Plan continue to inform how DOD will move towards achieving cyberspace superiority. Many of these tasks are defensive, directed at addressing the vulnerabilities of the DOD networks, and take into consideration the fact that the internet is a completely connected environment where both DOD and private networks reside.

In an interview on "60 Minutes," former Director of National Intelligence Michael McConnell said that "If I were an attacker and I wanted to do strategic damage to the United States…I would sack electric power on the U.S. East Coast, maybe the West Coast, and attempt to cause a cascading effect. All of those things are in the art of the possible from a sophisticated attacker." He was then asked whether he believes that adversaries have the ability to bring down the power grid, and he replied "I do." Crippling the U.S. power grid would not only cause catastrophic economic problems; presumably it would lead to significant loss of life, especially if the outage was prolonged. Likewise, it could cripple DOD's ability to generate and sustain forces.

15c) In light of our current vulnerability to cyber attack, what is the risk in your view that DOD and U.S. Cyber Command could be deterred from undertaking coercive action against countries such as Iran or North Korea because of the possibility that they could successfully launch devastating attacks on critical U.S. infrastructure?

(U) Answer provided in the classified supplement.

15d) Is this level of vulnerability consistent with the NMS-CO assertion that the U.S. ensures "superiority" in cyberspace?

(U) Yes, it is consistent that the United States seeks to ensure superiority in cyberspace: Even with the clear understanding that we could experience damage to our infrastructure, we must be prepared to "fight through" in the worst case scenario. Based on vulnerability, step one is to ensure that we *can* defend our networks. In fact, the use of the term superiority, versus dominance or supremacy, reflects the limits of our capabilities throughout the domain. Having recognized the gap between the end states of the NMS-CO and current capabilities, the Department developed an implementation plan to close these gaps. The current state of our networks presents a strategic vulnerability for the Department and the Nation. If confirmed, I will focus U.S. Cyber Command on securing the Department's networks and, as requested, assisting other Federal agencies to secure the networks for which they are responsible.

The NMS-CO states that "US law and national policy assign DOD three main roles: defense of the nation, national incident response, and critical infrastructure protection…Although partner departments and agencies have responsibilities to secure

portions of cyberspace, only DOD conducts military operations to defend cyberspace, the critical infrastructure, the homeland, or other vital US interests. If defense of a vital interest is implicated, DOD's national defense mission takes primacy even if that would conflict with, or subsume, the other support missions."

15e) Are these statements consistent with DOD's statements that U.S. Cyber Command will not have the mission to defend the ".gov" and ".com" networks?

(U) Yes, they are consistent. Although U.S. Cyber Command's mission will not include defense of the .gov and .com domains, given the integration of cyberspace into the operation of much of our critical infrastructure and the conduct of commerce and governance, it is the obligation of the Department to be prepared to provide military options to the President and SECDEF if our national security is threatened. Any defensive action in support of a domain other than .mil would require a proper request for assistance or a directive from the President.

15f) Has "critical infrastructure" been formally defined or otherwise identified for the purposes of cybersecurity?

(U) Yes, specifically "critical infrastructure" has been formally defined in HSPD-7 as those systems or assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

15g) Do these statements reflect current policy?

(U) Yes, they reflect current policy.

15h) Do these statements mean that DOD's mission to defend the nation "takes primacy" over the Department of Homeland Security's role in some situations?

(U) Yes, when war or any attack or other national security crisis arises whereby the use of force is contemplated, the DOD would take the lead in defending the nation. However, a Presidential order calling on DoD to take the lead role in responding to a cyber attack on the U.S. would be required before DOD assumes this lead role. I believe that DOD and DHS are completely in synch on this point.

The NMS-CO states that "under the authorities of the Secretary of Defense, DOD will use network exploitation to gather intelligence and shape the cyberspace environment as necessary to provide integrated offensive and defensive options." This statement appears to mean that DOD will attempt to gain access to foreign networks to create the ability to conduct offensive operations.

15i) Under what conditions would DOD prepare foreign networks for offensive operations when access is acquired for intelligence gathering?

(U) DOD conducts extensive planning for a wide range of contingencies including planning for cyberspace operations. Effective planning for offensive cyber operations requires extensive knowledge and understanding of foreign networks and is accomplished by foreign intelligence collection. Any preparation of foreign networks outside that is beyond the realm of intelligence gathering can only be conducted by lawful order (EXORD) from SECDEF and the President.

15j) Are such actions authorized and reported to Congress under Title 10 or Title 50?

(U) Preparation of foreign networks for offensive operations is authorized only when part of a SECDEF-approved military operation under Title 10 of the United States Code; such military operations are subject to congressional armed services committee oversight. Foreign intelligence collection activities are subjected to Congressional intelligence oversight.

15k) Does the Secretary of Defense have the unilateral authority to direct intelligence-gathering operations in cyberspace?

(U) The Secretary of Defense, as authorized by law and executive order, can direct intelligence activities in cyberspace for those intelligence activities, such as SIGINT, under his operational control.

15l) If the Secretary of Defense is the President's executive agent for signals intelligence, what is the role of the Director of National Intelligence in directing signals intelligence collection in cyberspace?

(U) The DNI provides the National Intelligence Strategy and the National Intelligence Priority Framework, among others, to the entire intelligence community. The DNI also plays a role with respect to resource allocation via the National Intelligence Program.

15m) Under the Secretary's role as the executive agent for signals intelligence, what was the Secretary's responsibility for the policy decisions regarding the NSA's Terrorist Surveillance Program, and the assistance that NSA is providing to the Department of Homeland Security through the Einstein 3 intrusion detection and prevention program?

(U) Answer provided in the classified supplement.

The NMS-CO states that "Adversaries are deterred from establishing or employing offensive capabilities against US interests in cyberspace. DOD will deter malicious adversary use of cyberspace, while promoting freedom of action and trust and confidence in US cyberspace operations. Through deterrence, DOD seeks to influence the adversary's

decision-making processes by imposing political, economic, or military costs; denying the benefits of their actions; and inducing adversary restraint based on demonstrated US capabilities."

15n) In your opinion, is it the case that "adversaries are deterred" from acting against U.S. interests in cyberspace?

(U) Answer provided in the classified supplement.

15o) Does the United States have a deterrence doctrine and a deterrence strategy for cyber warfare?

(U) Answer provided in the classified supplement.

15p) Has the U.S. ever "demonstrated capabilities" in cyberspace in a way that would lead to deterrence of potential adversaries?

(U) Not in any significant way. We have conducted exercises and war games, and responded to threats, intrusions, and even attacks against us in cyberspace. Law Enforcement and the Counter-Intelligence community have responded to intrusions and insider threats. Even industry and academia have attempted to "police" the Internet. How all of these have deterred criminal actions, terrorists, hostile intelligence entities, and even nation states cannot be systematically measured.

16. <u>Implications of U.S. Dependence on Cyber Networks</u>

Many experts assert that the U.S. is the most vulnerable country in the world to cyber attack because we are the most networked nation and the one that has most fully exploited computer networks for business, government, and military functions. This judgment implies that the United States has the most to lose in a serious cyber conflict.

16a) How could DOD best compensate for U.S. dependence on vulnerable cyber networks in developing effective deterrent strategies?

(U) Answer provided in the classified supplement.

16.b) Given U.S. vulnerabilities, is it in our interest to engage in certain kinds of offensive cyber warfare, and possibly set precedents by example that other nations might follow?

(U) Answer provided in the classified supplement.

17. Covert Action Versus Traditional Military Operations

What is your understanding of whether clandestine offensive actions in cyberspace conducted by DOD in connection with an ongoing military conflict where the hand of the U.S. Government is intended to be concealed "covert action" under the law, or are they considered traditional military operations?

(U) Covert action, as defined by law, includes "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly." The law goes on specifically to except "traditional … military activities" from being considered covert actions. (50 USC 413b(e)(2000)) Traditional military activities are often clandestine in order to guarantee mission success and protect tactics, techniques, and procedures – this is no different in cyberspace. DOD believes the traditional military activities exception applies to the emerging field of cyberspace operations.

17a) Does it matter whether such actions are conducted within or outside of a theater of ongoing, traditional armed conflict?

(U) This is a matter of ongoing debate. Proposed actions to deliver effects to Combatant Commanders at the tactical and operational level should be pursued as traditional military operations, under existing authorizations, if possible. Any actions that we take must be approved by the Secretary of Defense and the President through a lawful order.

18. Requirement for Transit Rights

Under international law, nations enjoy sovereign rights over the territorial extent of their countries and the airspace above it, although not in space. Transiting that sovereign territory and airspace for military purposes requires permission.

18a) In a situation where a government intends to deliver a cyber weapon or capability to a country not adjacent to its territory, through terrestrial telecommunications networks, what is the legality of doing so without the permission of the governments of the nations through which the weapon must pass?

(U) Answer provided in the classified supplement.

19. The Challenge of Attribution

An essential feature of military, intelligence, and criminal or malicious activities in cyberspace is the ease with which the origin and the identity of those responsible for an attack can be concealed. This "attribution" problem is severe. If it is impossible to say with certainty who committed an attack, no one can be held responsible, making deterrence and retaliation alike problematic. The attribution capabilities that do exist

appear to be time- and resource-intensive, which can make appropriate, timely responses difficult or even impossible.

19a) How can deterrence be established in the absence of reliable attribution?

(U) I agree that attribution can be very difficult. We must approach this problem in two ways. First and foremost, the most effective way to deter adversaries is to increase the security of our own networks. This will act as a deterrent to those adversaries who target the United States simply because we are an easy mark. This is a national problem and better security solutions must be encouraged for all U.S. public and private networks.

(U) Concurrently, we must partner closely with the intelligence community to improve our ability to determine attribution. We must also establish partnerships with nation-states that share common goals for lawful behavior in cyberspace. Such agreements would establish expectations of normative behavior for cyber activities and thresholds for bad behaviors that would not be allowed to continue. Such expectations will require standards of evidence that are mutually acceptable and include highly automated procedures that allow attacks to be alerted on and halted quickly.

(U) Criminal law models depend on deterrence, as well. Legal scholars have argued that crimes that often go unsolved (vandalism, for example) should be punished more harshly to ensure an effective example is offered in the few cases when it's available. Under this model, the US should take swift and effective action in every case in which it can attribute an offensive action to a particular adversary.

(U) Attribution has been a problem since the beginning of the terrorism era. For example, in 1983 when the Marine barracks in Beirut was bombed, the US would likely have taken strong action against the perpetrator – but the perpetrator was dead and the planners were unknown. This problem continues today in kinetic operations as well as in cyber.

(U) The bottom line is, the only way to deter cyber attack is to work to catch perpetrators and take strong and public action when we do.

19b) What authorities are required, or what procedures must be invoked, to track back through layers of an attack involving computers located in the United States and owned by U.S. persons?

(U) Investigations of cyber attacks originating or appearing to originate from the United States are typically law enforcement investigations and a law enforcement warrant is used to attempt to track back through layers involving computers located in the United States or owned by U.S. persons. If there is reason to believe that the attack is being conducted by a foreign power or agent of a foreign power, though appearing to originate from the United States, the investigation can be a counter intelligence investigation and the Foreign Intelligence Surveillance Act order would be used to track back through layers involving computers located in the United States or owned by a U.S. person.

19c) What are the legalities, both in domestic and international law, involved in "shooting back" immediately at the sources of a large-scale attack, with and without a determination that the sources are commandeered computers?

(U) A commander's right to general self-defense is clearly established in both U.S. and international law. Although this right has not been specifically established by legal precedent to apply to attacks in cyberspace, it is reasonable to assume that returning fire in cyberspace, as long as it complied with law of war principles (e.g., proportionality), would be lawful.

(U) Remainder of answer provided in the classified supplement.

The law regarding self-defense in the case of an attack has never required a determination of identity before action can be taken. For example, if someone is shooting at you, it isn't necessary to establish what his name is before shooting back. If someone in a car is trying to run down a police officer, the officer is not required to determine whether the car is stolen before shooting out the tires in self-defense. Similarly, the fact that computers may be commandeered is irrelevant to the exercise of self-defense.

The United States has always hoped that the Internet would play a "subversive" role in countries with authoritarian governments.

19d) If the U.S. government takes vigorous diplomatic action, as some experts recommend, to establish the norm that governments are responsible for what happens in cyberspace within their sovereign domains as a way to deal with the attribution problem, is there a danger we could be providing a strong justification for governments abroad to intensify surveillance and increase government controls on the Internet?

(U) Governments that have a tendency to curtail the freedoms of their citizens will likely take such actions regardless of U.S. policies regarding cyberspace. However, the United States has the opportunity to model for other nations the process by which a nation-state can allow freedom of expression, and even advanced concepts such as Net Neutrality, and still insist on cyberspace behaviors that meet the norms of international expectations in that they could not be construed as constituting an attack in cyberspace. We can do this without increased individual surveillance.

19e) Is it accurate that a large proportion of world-wide unauthorized cyber intrusions and malicious cyber activity originates or appears to originate within the United States?

(U) Answer provided in the classified supplement.

19f) Is it reasonable to hold other governments responsible for all such activity originating in their countries if the United States government cannot or will not stop it here?

(U) Every government is responsible for actions originating in its own country. We make every effort to address activity originating in the United States, and we expect other countries will do the same.

20. <u>Title 10 Versus Title 50 Reporting and Oversight</u>

As the attached solicitations and program descriptions indicate, and the National Military Strategy for Cyberspace Operations implies, gaining access to a cyberspace target for the purpose of collecting intelligence also provides the basis for attacking that target, and vice versa. Intelligence collection in cyberspace is authorized and overseen under Title 50 procedures, whereas operational preparation of the environment for military action is authorized and overseen under Title 10 procedures.

20a) Has the administration determined how it is going to authorize these actions and report them to Congress?

(U) Intelligence collection in cyberspace is conducted as part of a foreign intelligence mission and is subject to congressional intelligence oversight; e.g., the SIGINT Computer Network Exploitation (CNE) mission is conducted in accordance with SIGINT procedures and is reported to the intelligence oversight committees. Military actions in cyberspace done to prepare the environment for possible cyber attack are authorized through SECDEF Execute Orders and reportable to the Armed Services Committees.

The attached solicitations and program descriptions indicate that non-intelligence elements of DOD are developing capabilities to penetrate foreign networks clandestinely, remain there undetected, and exfiltrate data secretly.

20b) Are non-intelligence elements of DOD authorized to collect intelligence in cyberspace through the clandestine penetration of networks?

(U) Non-intelligence elements of the DOD are not authorized to collect intelligence or conduct preparation of the environment without an appropriate execute order.

21. <u>Systems Acquisition</u>

Combatant Commands by design play a restricted role in the acquisition process. However, the Commander, U.S. Cyber Command, is to be dual-hatted as the Director of NSA, which is a large enterprise with substantial resources for developing, procuring, and supporting new equipment, systems, and capabilities. In addition, the Commander will

exercise operational control of Defense Information Systems Agency (DISA) networks, which also acquires systems and capabilities.

(U) Commander, U.S. Cyber Command will not exercise command or operational control over the Defense Information Systems Agency communications networks. DISA will continue to be responsible for acquiring, engineering and provisioning enterprise infrastructure to assure the availability of military information networks. As a Combat Support Agency, DISA will maintain a close working relationship with U.S. Cyber Command, providing expertise on the networks, communications and computing infrastructure operated by DISA through both a DISA Field Office and a DISA Support Element.

21a) Is there a precedent for a Combatant Commander to exercise this degree of direct control over acquisition organizations, aside from Special Operations Command, which Congress expressly provided with acquisition authority?

(U) Commander, U.S. Cyber Command, would depend upon the Military Departments and Agencies to deliver on U.S. Cyber Command-documented requirements for capabilities. Each of the Military Departments and Agencies has oversight to ensure that this is done properly. This is consistent with other Combatant and Sub-Unified Commands, with the exception of U.S. Special Operations Command.

21b) What measures is the Department taking to guarantee that Commanders of U.S. Cyber Command do not circumvent the requirements process and the established acquisition process by directing subordinates at NSA or DISA to directly address needs perceived by Cyber Command?

(U) U.S. Cyber Command will be a separate organization with a separate and distinct acquisition authorities/process and staff from the NSA and DISA. The separate oversight, accountability chains, and the ability to audit actions taken by the two distinct organizations of NSA and the future U.S. Cyber Command exist to ensure that the Commander, U.S. Cyber Command follows the Cyber Command requirements process and that the Director of NSA follows the established NSA acquisition process. Specifically, NSA and U.S. Cyber Command will have separate staffs with distinct authorities and oversight. U.S. Cyber Command will operate under the same authorities and oversight as other Combatant Commands and Sub-Unified Commands.

(U) NSA must operate under the authority and oversight of DOD and Director, National Intelligence. Operating under distinct authorities is not a new condition for the Director of NSA. I, like all the DIRNSAs before me, am used to working under distinct authorities (Title 10 and Title 50) and oversight (DOD and DNI), because of NSA's two separate missions in Foreign Intelligence and Information Assurance.

(U) Furthermore, as Director of NSA, I have delegated acquisition authority to the Senior Acquisition Executive (SAE), who is not assigned to or aligned with U.S. Cyber Command. The SAE position was established in response to recommendations by

Congress in 2000. Additionally, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)) and the Office of the Director of National Intelligence (ODNI) both have Milestone Decision Authority (MDA) for some NSA Major System Acquisitions (MSA). While ODNI and USD(AT&L) have delegated the NSA SAE Milestone Decision Authority for certain major acquisition programs through the annual delegation process, they retain joint acquisition oversight over all major system acquisitions. Both organizations conduct quarterly reviews of all MSA / Acquisition Category I and Special Interest Programs, and USD(AT&L) conducts a tri-annual review of NSA's contracting process in accordance with the Defense Financial Acquisition Regulation Supplement.

(U) The Director of DISA reports to ASD(NII) and will not be a subordinate of Commander, U.S. Cyber Command. Additionally, Commander, U.S. Cyber command will have no subordinates in DISA.

22. <u>Extended Deterrence in Cyberspace</u>

22a) With respect to close allies who depend upon the United States for their security, will DOD provide a defense capability against attacks on their critical military, government, and economic infrastructure?

(U) Answer provided in the classified supplement.

22b) Is DOD considering an "extended deterrence" model similar to that which we have offered through the U.S. "nuclear umbrella"?

(U) I am not aware of any efforts to develop an extended deterrence model for cyber.

The financial sector in the United States is tightly integrated with and dependent upon the global financial network, such that a massive attack on financial networks abroad would probably inflict great harm on the United States.

22c) To what extent does DOD consider that the defense of some U.S. critical infrastructures must encompass network extensions abroad?

(U) Answer provided in the classified supplement.

23. <u>Authorities and Procedures for Investigating ".mil" Intrusions</u>

One of the difficult issues confronting the Einstein 3 intrusion detection and prevention program is what to do when packets are detected that contain malicious code. Attackers usually act indirectly against their targets, routing attacks through a series of innocent intermediaries to hide their identities and locations. A malicious penetration or attack on a ".gov" computer or network may be launched from a specific computer but without the knowledge of the legitimate owner of that computer. However, government

personnel discovering such an attack have no way of knowing, without further investigation, which computer owners in a chain may be complicit. The Federal Government has not announced how it will specifically respond in terms of investigating actual or apparent attacks, retaining and analyzing associated data, when a warrant is required, and so forth, for the defense of the civil ".gov" networks. However, the Department of Defense has already fielded intrusion detection and prevention capabilities developed by the National Security Agency at the gateways to the ".mil" networks.

23a) Does this mean that the Department has developed and received approval for protocols and procedures for investigating U.S. persons whose computers may be implicated in attacks on ".mil" targets?

(U) Answer provided in the classified supplement.

24. <u>Explaining Cybersecurity Plans to the American People</u>

The majority of the funding for the multi-billion dollar Comprehensive National Cybersecurity Initiative (CNCI) is contained in the classified National Intelligence Program budget, which is reviewed and approved by the congressional intelligence committees. Almost all important aspects of the CNCI remain highly classified, including the implementation plan for the Einstein 3 intrusion detection and prevention system. It is widely perceived that the Department of Homeland Security is actually likely to simply extend the cyber security system that the NSA developed for DOD into the civilian and even the private sector for defense of critical infrastructure. DOD is creating a sub-unified Cyber Command with the Director of NSA as its Commander.

24a) In your view, are we risking creating the perception, at home and abroad, that the U.S. government's dominant interests and objectives in cyberspace are intelligence- and military-related, and if so, is this a perception that we want to exist?

(U) No, I don't believe we are risking creating this perception as long as we communicate clearly to the American people – and the world – regarding our interests and objectives.

24b) Based on your experience, are the American people likely to accept deployment of classified methods of monitoring electronic communications to defend the government and critical infrastructure without explaining basic aspects of how this monitoring will be conducted and how it may affect them?

(U) I believe the government and the American people expect both NSA and U.S. Cyber Command to support the cyber defense of our nation. Our support does not in any way suggest that we would be monitoring Americans.

(U) I don't believe we should ask the public to accept blindly some unclear "classified" method. We need to be transparent and communicate to the American people about our objectives to address the national security threat to our nation – the nature of the threat, our overall approach, and the roles and responsibilities of each department and agency involved – including NSA and the Department of Defense. I am personally committed to this transparency, and I know that the Department of Defense, the Intelligence Community, and rest of the Administration are as well. What needs to remain classified, and I believe that the American people will accept this as reasonable, are the specific foreign threats that we are looking for and how we identify them, and what actions we take when they are identified. For these areas, the American people have you, their elected representatives, to provide the appropriate oversight on their behalf.

(U) Remainder of answer provided in the classified supplement.

24c) What are your views as to the necessity and desirability of maintaining the current level of classification of the CNCI?

(U) In recent months, we have seen an increasing amount of information being shared by the Administration and the departments and agencies on the CNCI and cybersecurity in general, which I believe is consistent with our commitment to transparency. I expect that trend to continue, and personally believe and support this transparency as a foundational element of the dialogue that we need to have with the American people on cybersecurity.

25) Military Service Roles in Cyber Command

Each of the military services is planning to create new organizations and structures, or expand existing ones, to support the new U.S. Cyber Command. However, cyberspace is a virtual realm, considerably removed from the physical world.

25a) Has the Department undertaken any analyses of alternative means of providing forces and capabilities to the new Command?

(U) In accordance with the SECDEF memorandum directing the establishment of U.S. Cyber Command, each of the Services conducted a thorough mission analysis on how best to provide capabilities to U.S. Cyber Command, selected a course of action for the near term, and briefed that selection to the Deputy Secretary.

(U) Further, U.S. Strategic Command, in coordination with the Services and other combatant commanders, completed a study last year that gives us an initial vector for required force size and composition for a portion of the force. To that end, the Joint Requirements and Oversight Committee approved that recommendation and directed a more in-depth study. The study, the Cyber Analysis Campaign, is underway and should give us a force sizing construct by the end of the summer.

25b) Can it be said that there is a logical basis for ground, sea, and air components in cyberspace – apart from the fact that each of the services operate networks that must be defended?

(U) There is a logical basis for the department to organize both efficiently and consistently to achieve its assigned mission. In much the same manner that – from a mission standpoint – special operations or logistics crosses all warfighting dimensions, so does cyberspace. There may come a time when this would merit further consideration based upon lessons to be learned. Currently, the Military Departments organize, man, train, and equip to generate and sustain mission capacity on behalf of the nation. Like other operational commands, it will be U.S. Cyber Command's business to take this cyber capacity – built to a common standard – and turn that into joint, combined cyber capability to achieve the supported commander's assigned mission as authorized by the Secretary of Defense.

25c) Is it optimal that each service have a separate organization for supporting U.S. Cyber Command, especially in the areas of intelligence and offensive cyber warfare?

(U) Yes, I believe so. If cyberspace was homogenous and the entirety of the work force did the same job, one could make the argument that the Department doesn't need each Service to have its own cyber component. But that would be a vast oversimplification of the complexity of the domain. At the operational and tactical levels of war, the Service components will be responsible for significant cyber operations. They will depend upon the networks for command and control of their forces and must be able to defend those networks. Over time the Services will also bring resources to bear in the intelligence and offensive cyber realm that will support their component missions at the operational and tactical levels of war, with deconfliction by U.S. Cyber Command. Each Service brings a unique perspective and some specialized capability to the fight that would be neither efficient nor effective to flatten into a singular whole. In cyberspace, as in all the domains, each Service brings capability to be employed in the combined arms philosophy that makes the whole greater than the sum of the parts.

26. <u>Command of National Defense in Cyberspace</u>

A cornerstone of military doctrine is the importance of unity of command, particularly in time-sensitive scenarios such as those that are likely to arise in cyberspace. In the federal government, the Department of Homeland Security is in charge of defending the country against cyber attacks, but authorities and responsibilities are fragmented and spread across the Intelligence Community, the Department of Defense, the Department of Homeland Security, the Justice Department, the Treasury Department, and the Department of Energy. Also, each department and independent agency is responsible for operating and equipping its own networks.

26a) In your opinion, is there adequate unity of command and authorities for the nation's response to serious cyber attacks?

(U) Unity of command within DOD is being improved with the establishment of U.S. Cyber Command; however, unity of effort, vice command, is equally important and achievable since effective cyber security requires a whole-of-government approach.

(U) As securing and defending our national cyber interests is an evolving work in progress, coordination, cooperation, and information sharing across the Federal Government is paramount. A rigorous partnership with DHS -- as they look to secure and protect the .gov domain and critical infrastructure -- is particularly crucial.

(U) DOD continually reviews its existing authorities and directives to determine what, if any, changes need to be requested to support ongoing or contingency plans. Our unique challenge in this domain is to develop a thorough understanding of the domain, posture to be prepared to recognize as rapidly as possible those vulnerabilities or threat unknowns and set effective "post-crisis" frameworks and conditions for decision makers, policy makers, and legislators pre-crisis.

26b) If not, what is the process and schedule for defining and establishing an effective construct?

(U) Ultimately, the best processes and policies are those that enable our national decision makers and operating forces to achieve the best desired outcome. DOD continues to support and help protect our national cyber interests as authorized and directed.

Designing the Internet for Better Security

Cyber security experts emphasize that the Internet was not designed for security.

27a) How could the Internet be designed differently to provide much greater inherent security?

(U) The design of the Internet is – and will continue to evolve – based on technological advancements. These new technologies will enhance mobility and, if properly implemented, security. It is in the best interest of both government and industry to consider security more prominently in this evolving future internet architecture. If confirmed, I look forward to working with this Committee, as well as industry leaders, academia, the Services, and DOD agencies on these important concerns.

27b) Is it practical to consider adopting those modifications?

(U) Answer provided in the classified supplement.

27c) What would the impact be on privacy, both pro and con?

(U) Answer provided in the classified supplement.

28. Congressional Oversight

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

28a) Do you agree, if confirmed for this high position, to appear before this Committee and other appropriate committees of the Congress?

Yes.

28b) Do you agree, when asked, to give your personal views, even if those views differ from the Administration in power?

Yes.

28c) 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, U. S. Cyber Command?

Yes.

28d) 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?

Yes.

28e) 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 the Committee regarding the basis for any good faith delay or denial in providing such documents?

Yes.