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. 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 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. Oversight

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.

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

(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. Authorities of Commander, U.S. Cyber Command

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. Deterrence and Escalation Control

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?