Advance Questions for Vice Admiral Michael S. Rogers, USN
Nominee for Commander, United States Cyber Command

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.

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

The integration of joint capabilities under the Goldwater-Nichols Act has been remarkable. All the warfighting benefits we enjoy from fighting as a joint force in air, land, sea – we are extending to cyberspace. In addition, it has improved civilian oversight of the Department of Defense (DoD) and fostered our military success over the last generation. Today U.S. military forces are more interoperable than ever before, and they set a standard for other militaries to attain. I see no need to modify the Goldwater-Nichols Act at this time.

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

I do not believe modifications to the Goldwater-Nichols Act are currently needed.

Duties

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

The Commander, U. S. Cyber Command (USCYBERCOM) is responsible for executing the cyberspace missions specified in Section 18.d.(3) of the Unified Command Plan (UCP) as delegated by the Commander, U.S. Strategic Command (USSTRATCOM) to secure our nation's freedom of action in cyberspace and to help mitigate risks to our national security resulting from America's growing dependence on cyberspace. Subject to such delegation and in coordination with mission partners, specific missions include: directing DODIN operations, securing and defending the DODIN; maintaining freedom of maneuver in cyberspace; executing full-spectrum military cyberspace operations; providing shared situational awareness of cyberspace operations, including indications and warning; integrating and synchronizing of cyberspace operations with combatant commands and other appropriate U.S. Government agencies tasked with defending the our nation’s interests in cyberspace; provide support to civil authorities and international partners. All these efforts support DoD’s overall missions in cyberspace of defending the nation against cyber attacks, supporting the combatant commands, and defending Department of Defense networks.

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

I am humbled and deeply honored that the President has nominated me to be the second Commander of USCYBERCOM and the seventeenth Director of the National Security Agency (NSA). Over the past three decades, I have served in a wide variety of Joint and Navy positions that have prepared me well for the challenges ahead if confirmed by the U.S. Senate.

First, I have more than 32 years in the profession of arms, serving in various command, staff, and intelligence positions afloat and ashore. I have been the director for Intelligence for both the Joint Chiefs of Staff and U.S. Pacific Command, special assistant to the Chairman of the Joint Chiefs of Staff, and commanded at multiple levels. I have over 27 years of dedicated experience in the SIGINT arena as an Information Warfare Officer and have held significant responsibilities in the cyber arena for much of the past 12 years.

In particular, my experiences and knowledge gained over the last two and a half years while serving as Commander of both Fleet Cyber Command and Tenth Fleet have done much to prepare me for the challenges of this new complex warfighting domain that is cyberspace. I should note that my responsibilities there include the command of the U.S. Navy's cryptologic capabilities, and so I have seen firsthand the relationship between cryptology and cybersecurity, and the importance of partnerships with interagency capabilities, with our allies, and with industry to strengthen the defense of our collective networks. My service at Fleet Cyber Command/Tenth Fleet afforded me direct experience, particularly in the realm of deliberate and crisis action planning, to ensure the effective execution of cyberspace responsibilities as directed by the Secretary of Defense through the Commander, USSTRATCOM.

Finally, my academic background has also helped prepare me for the challenges of high-level command, national security decision making, and international engagement. I hold a Master of Science in National Security Strategy and am a graduate of both the National War College and the Naval War College. I was also a Massachusetts Institute of Technology Seminar XXI fellow.

Does the Commander of U.S. Cyber Command have command of or exercise operational control of the Defense Information Systems Agency's and military services' communications networks?

If confirmed as Commander, USCYBERCOM, I will be responsible for directing the operation and defense of DoD's information networks as specified in the Unified Command Plan and as delegated by Commander, USSTRATCOM. The Defense Information Systems Agency (DISA) provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to national leaders, joint warfighters, and other mission and coalition partners across the full spectrum of operations. As a Combat Support Agency, DISA maintains a close working relationship with USCYBERCOM, providing expertise on the networks, communications and computing infrastructure that it operates. I will not exercise command or operational control over DISA communications networks.

As a career intelligence officer, what qualifications do you have to command these networks?

As noted in my biography, much of my career has involved not only intelligence duties but the command, administration, use, and employment of information networks and the data they carry, process, and store to protect and guard our nation. Over the course of my services, I have witnessed and helped further the revolution in information technology that has helped make our military second-to-none in its ability to communicate and control forces while providing decision-makers with unprecedented situational awareness. I have also devoted a great deal of my service to understanding and mitigating the vulnerabilities that our dependence on information networks can create for our military and our nation. In my current duties as Commander, Fleet Cyber Command I exercise operational control over Navy's networks and have done so for 30 months.

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

As noted above, I have exercised command previously at both junior and senior levels. I currently command Fleet Cyber Command and Tenth Fleet, a global team of nearly 15,000 men and women. Their operating environment is dynamic, and demanding; Fleet Cyber Command/Tenth Fleet has literally been "in action" against capable and determined adversaries seeking access to our networks since the day I assumed command in 2011. The planning and operations we have conducted to protect our networks and provide the Navy and our military and government freedom of maneuver in cyberspace have been complex.

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?

Any individual can learn more to enhance his or her expertise and abilities, and I have found that truth amply applies to me in understanding the very complex and rapidly evolving domain that is cyberspace. If confirmed, I shall meet with the Combatant Commanders to ascertain how USCYBERCOM can better support their missions. Additionally, I would engage with key officials and personnel within the Executive and Legislative branches of the United States government, leaders throughout the Intelligence Community, Law Enforcement, the Department of Homeland Security, and senior allied officials to hear their ideas about how we can work together to identify, assess, and mitigate the cyber threats we all face.

Relationships

Section 162(b) of title 10, United States Code, provides that the chain of command runs from the President to the Secretary of Defense and from the Secretary of Defense to the commanders of the combatant commands. Other sections of law and traditional practice, however, establish important relationships outside the chain of command. Please describe your understanding of the relationship of the Commander, U. S. Cyber Command, to the following officials:

The Secretary of Defense

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

The Deputy Secretary of Defense

In accordance with title 10, U.S.C., section 132, the Deputy Secretary of Defense performs such duties and exercises powers prescribed by the Secretary of Defense. The Deputy Secretary of Defense will act for and exercise the powers of the Secretary of Defense when the Secretary is disabled or the office is vacant. If confirmed, I will work closely with the Deputy Secretary, in coordination with Commander, USSTRATCOM.

The Director of National Intelligence

The Intelligence Reform and Terrorist Prevention Act of 2004 established the Director of National Intelligence to act as the head of the Intelligence Community, principal advisor to the President and the National Security Council on intelligence matters pertaining to national security, and to oversee and direct the implementation of the National Intelligence Program. Pursuant to title 50, U.S.C., section 403, subject to the authority, direction, and control of the President, the Director of National Intelligence coordinates national intelligence priorities and facilitates information sharing across the Intelligence Community. If confirmed, I will work closely with the Commander, USSTRATCOM and through the Secretary of Defense to coordinate and exchange information with the Director of National Intelligence as needed to ensure unified effort and synergy within the Intelligence Community in matters of national security.

The Under Secretary of Defense for Policy

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, USSTRATCOM, on all policy issues that affect USCYBERCOM operations.

The Under Secretary of Defense for Intelligence

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 shall work closely with the Under Secretary of Defense for Intelligence, in coordination with Commander, USSTRATCOM, on matters in the area of USCYBERCOM's assigned responsibilities.

The Under Secretary of Defense for Acquisition, Technology, and Logistics

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 shall work closely with the Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with Commander, USSTRATCOM, on matters in the area of USCYBERCOM's assigned responsibilities.

The Assistant Secretary of Defense for Homeland Defense

The Assistant Secretary of Defense for Homeland Defense executes responsibilities including overall supervision of the homeland defense and defense support of civil authorities activities of the DoD while serving under the Under Secretary of Defense for Policy. Any relationship the Commander, USCYBERCOM 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 shall work 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.

The Chief Information Officer

Under the authority of Department of Defense Directive 5144.02 and consistent with Titles 10, 40, and 44, U.S.C., the DoD Chief Information Officer (CIO) is the Principal Staff Assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on information resources management and position, navigation, and timing matters. The DoD CIO is tasked with improving the combat power of the Department—as well as its security and efficiency—by ensuring that the Department treats information as a strategic asset and that innovative information capabilities are available throughout all areas of DoD supporting war fighting, business, and intelligence missions. The DoD CIO is the Department's primary authority for the policy and oversight of information resources management, to include matters related to information technology, network defense, and network operations, and it also exercises authority, direction, and control over the Director, Defense Information Systems Agency. If

confirmed, I look forward to working closely with the Chief Information Officer through the Secretary and Deputy Secretary of Defense and Commander USSTRATCOM on matters in the area of USCYBERCOM's assigned responsibilities.

The Chairman of the Joint Chiefs of Staff

The Chairman is the principal military advisor to the President, National Security Council, and Secretary of Defense. Title 10, U.S.C, Section 163 allows communication between the President or the Secretary of Defense and the Combatant Commanders to flow through the Chairman. By custom and tradition, and as instructed by the Unified Command Plan, if confirmed, I would normally communicate with the Chairman in coordination with the Commander, U.S. Strategic Command.

The Secretaries of the Military Departments

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 clear but requires coordination with each Secretary to ensure there is no infringement upon those lawful responsibilities which a Secretary alone may discharge. If confirmed, I look forward to building a strong and productive relationship with each of the Secretaries of the Military Departments in partnership with Commander, U.S. Strategic Command.

The Chiefs of Staff of the Services

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

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

U.S. Cyber Command is a subordinate unified command under U.S. Strategic Command. The Commander, U.S. Cyber Command has both supported and supporting relationships with other combatant commanders, largely identified within the Unified Command Plan, the Joint Strategic Capabilities Plan, execute orders, and operation orders. In general, the Commander, U.S. Cyber Command is the supported commander for planning, leading, and conducting DoD defensive cyber and global network operations and, in general, is a supporting commander for offensive missions. Specific relationships with Commander, U.S. Northern Command will be delineated by the President or the Secretary of Defense in execute and/or operation orders. If confirmed, I

look forward to working with the combatant commanders to broaden and enhance the level and range of these relationships.

The Director of the Defense Information Systems Agency

The Defense Information Systems Agency (DISA) is a DoD Combat Support Agency that provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to national leaders, joint warfighters, 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. If confirmed, I shall work closely with the Director of DISA on matters of shared interest and importance.

Oversight

The resourcing, planning, programming and budgeting, and oversight for U.S. Cyber Command's missions is fragmented within the Defense Department, the executive branch as a whole, and within Congress. Section 932 of the National Defense Authorization Act (NDAA) for Fiscal Year 2014 requires the Secretary of Defense to appoint a Senate-confirmed official from the Office of the Under Secretary of Defense for Policy (USD(P)) to act as the principal cyber advisor to the Secretary.

What is your view of this legislation? Do you believe that it will improve oversight, planning, and resource allocation for the cyber mission within DOD?

I believe this legislation provides an opportunity to streamline cyber policy analysis and oversight within DoD, and its implementation will support DoD's long-term goals in cyberspace. Cyber is a complex issue that touches many parts of the Department and one single point of contact within the Office of the Secretary of Defense will reduce duplicative efforts and keep all offices that work on cyber issues in sync.

What changes to the legislation, if any, would you recommend?

I do not recommend any changes at this time. If confirmed, I can assure you that I will work closely with the principal cyber advisor selected by the Secretary of Defense.

Major Challenges and Problems

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

I believe the major challenge that will confront the next Commander, U.S. Cyber Command will be dealing with the changing threat in cyberspace. Adversaries today seek persistent presences

on military, government, and private networks for purposes such as exploitation and potentially disruption. We as a military and a nation are not well positioned to deal with such threats. These intruders have to be located, blocked, and extracted, sometimes over long periods of time. We have seen the extent of the resources required to wage such campaigns, the planning and intelligence that are essential to their success, and the degree of collaboration and synchronization required across the government and industry (and with our allies and international partners). We in DoD are creating capabilities that can adapt to these uses and others, but we have some key capability gaps in dealing with increasingly capable threats. Our legacy information architecture, for instance, is not optimized for defense in its current form, and our communications systems are vulnerable. U.S. military forces currently lack the training and the readiness to confront advanced threats in cyberspace. Finally, our commanders do not always know when they are accepting risk from cyber vulnerabilities, and cannot gain reliable situational awareness, neither globally nor in US military systems.

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

If confirmed, I plan to continue USCYBERCOM's current course of building cyber capabilities to be employed by senior decision-makers and Combatant Commanders. In accordance with the DoD *Strategy for Operating in Cyberspace*, USCYBERCOM with its mission partners and allies has been helping the DoD to build:

1. A defensible architecture;
2. Trained and ready cyber forces;
3. Global situational awareness and a common operating picture;
4. Authorities that enable action;
5. Doctrine and concepts for operating in cyberspace.

I would plan to assess these current priorities, which are DoD-wide, with an eye to shifting emphases across them as necessary and appropriate, and as computer and communication technologies continue to evolve.

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

USCYBERCOM is helping to accomplish something that our military has never done before. With the Services, allies, and a host of partners, it is putting in place foundational systems and processes for organizing, training, equipping, and operating military cyber capabilities to meet cyber threats. USCYBERCOM and the Services are building a world class, professional, and highly capable force in readiness to conduct full spectrum cyberspace operations. Its Cyber Mission Force is already engaged in operations and accomplishing high-value missions. It is no longer an idea on a set of briefing slides; its personnel are flesh-and-blood Soldiers, Marines, Sailors, Airmen, and Coast Guardsmen, arranged in military units. That progress is transforming potential capability into a reliable source of options for our decision makers to employ in defending our nation. Future progress in doing so, of course, will depend on our ability to field sufficient trained, certified, and ready forces with the right tools and networks to fulfill the growing cyber requirements of national leaders and joint military commanders. If confirmed, my

highest priority will be continuing and expanding this progress toward making USCYBERCOM capable of protecting our nation's freedom of maneuver in cyberspace.

The Fundamental Prospects for Defending Against Cyber Attacks

The ease with which nation-states, terrorists, and criminals, are able to penetrate corporations and government organizations to steal information suggests that the prospects for cyberdefense, using current techniques at least, are poor. Nonetheless, Cyber Command has been assigned the mission of defending the homeland, which at least implies that a defensive mission is practical and achievable. It may be possible to build resilience into critical infrastructure to recover from an attack, through back-up systems and redundant control systems that are less automated or electronically connected, but the government so far has not emphasized resilience over defense for our most critical infrastructure.

On a sustained basis in a conflict with a very capable nation-state, should we expect U.S. Cyber Command to be able to prevent cyber attacks from reaching their targets or causing great damage?

The U. S. possesses superior military might across all warfighting domains, cyberspace included. In truth, however, there has been no large scale cyber conflict yet in history, and the state of strategy and execution of cyber warfare is evolving as we speak. Our decision to collocate key intelligence operations and cyberspace capability serves as a force multiplier, if properly authorized and supported by policy, resources, and willpower. Our force construct is such that it provides the United States the flexibility to engage, both offensively and defensively, in specific areas of hostility or on a transnational basis. We are building or further developing our international partnerships and relationships for mutual support and recognition of norms of behavior. We know there are other nation-states who have equal or near-equal capability to ours; we have to be sure that we have the capabilities, processes, authorities, and, where appropriate, delegation and pre-approvals in place to prevent and respond to malicious activity. In a conflict where risk to our systems, information, and critical infrastructure was in play, that the U. S. would need to optimize our ability to see, block, and maneuver against attackers in a streamlined and efficient fashion. We still have significant work to do to build out our forces and capabilities. However, given the circumstances, yes, I believe it is realistic to expect that U. S. CYBERCOM could effectively engage the adversary to prevent attacks and severe damage.

Is it reasonable to expect the private sector nonetheless to build defenses to prevent serious impacts on critical infrastructure?

Yes. I believe that mission assurance and the protection of our critical infrastructure is an inherent obligation of all, not just DoD, DHS, DOJ/FBI and our government. In many cases, mission assurance relies on the provision, management, or facilitation of critical infrastructure lies in the private sector. Defensive measures could include not just automated capabilities to prevent or respond, but also adherence to proper standards of network security, administration, sharing of threat and vulnerability information, and compliance. These are as critical to

protection of infrastructure as is military or cyber might. In almost any scenario, collaboration and information sharing across private and public, governmental and non-governmental organizations will be a key to successful outcomes.

In your view, could such cyber attacks be prevented through the development of offensive capabilities and the principles of deterrence?

Yes, the development of both offensive and defensive capabilities can serve to deter an adversary from cyber attack. Strong capabilities can deter an attack by preventing an adversary from achieving his objectives and demonstrating the ability to impose costs on the adversary.

Should we expect U.S. Cyber Command to be able to prevent the more limited attacks that could be expected from powers with lesser cyber capabilities, such as North Korea and Iran?

Adversarial activities over recent years have shown that the level of expertise required to conduct potentially damaging operations has steadily lowered, enabling less capable actors to achieve some level of effect. Although we continue to build and develop our forces and capabilities, I believe that CYBERCOM has the capability to prevent such attacks, yes, whether from a capable or less capable adversary, given the order and provided that the supporting policies, authorities, relationships, and will to act are in place.

In your view, can cyber warfare capabilities provide an asymmetric advantage for such rogue nations, providing them the potential to strike the American people and economy?

Yes. Regardless of the target - assuming that the adversary has somehow developed the access - the physics of the cyberspace domain and the technology supporting it make it easier for an adversary to hide or obfuscate his capability, attack vector, and location, and deliver an effect on his target either singularly or repeatedly within milliseconds. If he or she has subverted any number of proxies from which to operate, that further multiplies the advantage enjoyed. When the victim is placed in a reactive posture by processes which constrain the ability to respond, the advantage is multiplied. Internal defensive measures can mitigate that advantage to an extent, of course.

If so, how should we demonstrate or clarify our retaliatory capability as a means of contributing to deterrence? Should the U.S. Government be more forthcoming about the nature of cyber warfare, and the balance between offensive and defensive capabilities?

I believe the recent disclosures of a large portion of our intelligence and military operational history may provide us with opportunity to engage both the American public and our international partners in discussion of the balance of offense and defense, the nature of cyber warfare, norms of accepted and unacceptable behavior in cyberspace, and so forth.

Support to Civil Authorities

U.S. Cyber Command has 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.

Please describe the ways that U.S. Cyber Command should assist civil authorities and the capability of U.S. Cyber Command to provide that assistance.

I believe that a request for support to civil authorities for cyber related assistance normally occur as a response to a Request for Assistance (RFA) from the Department of Homeland Security to DoD, and in close coordination with the Commanders of U. S. STRATCOM and U. S. NORTHCOM. That support could be technical assistance in a number of different ways, such as recommendations for improved network configurations, information assurance measures, or specific defensive response actions. Other technical assistance could be in the form of mitigation options, forensics, or data analysis.

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

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

Depending on the nature of the national emergency or crisis, and the requirement for cybersecurity support, SECDEF would determine which combatant commander would be supported and supporting and U. S. CYBERCOM would comply with that determination. In any scenario with respect to cyber security support to civil authorities, a close collaborative relationship between US Northern Command and US Cyber Command will be key.

Use of Force in Cyberspace

Does the Defense Department have a definition for what constitutes use of force in cyberspace, and will that definition be the same for our activities in cyberspace and those of other nations?

DoD has a set of criteria that it uses to assess cyberspace events. As individual events may vary greatly from each other, each event will be assessed on a case-by-case basis. While the criteria we use to assess events are classified for operational security purposes, generally speaking, DoD analyzes whether the proximate consequences of a cyberspace event are similar to those produced by kinetic weapons.

As a matter of law, DoD believes that what constitutes a use of force in cyberspace is the same for all nations, and that our activities in cyberspace would be governed by Article 2(4) of the U.N. Charter the same way that other nations would be. With that said, there is no international consensus on the precise definition of a use of force, in or out of cyberspace. Thus, it is likely

that other nations will assert and apply different definitions and thresholds for what constitutes a use a force in cyberspace, and will continue to do so for the foreseeable future.

Has the Defense Department, 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?

It is up to the President to determine when, based upon the circumstances of any event, including a cyberspace event, and the contemplated response that the President intends to proceed with, what consultations and reports are necessary to Congress, consistent with the War Powers Act.

The United States would evaluate its individual self-defense rights, as well as the self-defense rights of other nations, consistent with international law and Article 51 of the U.N. Charter. This analysis would assess whether an illegal use of force had occurred, and whether a state's inherent right of self-defense was triggered. If the United States held a collective defense obligation to the state that was subject to the illegal use of force, then the United States would evaluate its obligations consistent with its treaty obligations, keeping in mind that the U.N. Charter recognizes a state's inherent right of individual and collective self-defense. After all, collective self-defense obligations apply when another state is threatened or subject to a use of force in the cyber domain just as they would in other warfighting domains.

Could U.S. Cyber Command 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 behind the attack (i.e., a foreign government or non-state actors)? Without confident "attribution," under international law, would the Defense Department have the authority to "fire back" without first asking the host government to deal with the attack?

International law does not require that a nation know who is responsible for conducting an armed attack before using capabilities to defend themselves from that attack. With that said, from both an operational and policy perspective, it is difficult to develop an effective response without a degree of confidence in attribution. Likely, we would take mitigating actions, which we felt were necessary and proportionate, to defend the nation from such an attack. I'd note that in such an event, U.S. Cyber Command would be employing cyber capabilities defensively, in the context of self-defense.

Policies Governing Access to Sensitive Targets For Intelligence Collection and Targeting

Traditionally, espionage has not been regarded as a use of force or an act of war. However, 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 were detected, the victim may not know whether the purpose of the activity would be limited to espionage only, or would also constitute preparation for an attack.

Are there classes of foreign targets that the U.S. Government considers should be "off-limits" from penetration through cyberspace?

My view is that the U.S. Government should only conduct cyberspace operations against carefully selected foreign targets that are critical to addressing explicitly stated intelligence and military requirements, as approved by national policymakers and the national command authority.

Would or should such targets be immune to penetration by the United States in peacetime even for intelligence collection? Should there be a review process outside of DOD for such potential targets?

Intelligence collection is conducted in response to specific needs expressed by policy makers and military commanders for information. Those needs are vetted through a formal requirements process managed by the Director of National Intelligence that includes a review of sensitive policy equities.

How does the NSA currently consider these issues when making decisions about targeting for intelligence collection?

NSA conducts intelligence collection operations in response to specific requirements that are vetted through a formal process managed by the Director of National Intelligence. That process includes an interagency review of sensitive policy equities.

What role do the White House and the interagency coordination process play in this decision process?

The White House and the interagency community are directly involved in approving foreign intelligence requirements and determining what targets are appropriate for cyberspace and other Signals Intelligence operations. All cyberspace operations conducted by NSA and USCYBERCOM are governed by the policy constraints set by the White House and the interagency coordination process. President Obama recently announced improvements to this process in Presidential Policy Directive PPD-28.

NSA and USCYBERCOM (under its delegated intelligence authorities) conduct intelligence collection operations in response to specific requirements that are vetted through a formal process managed by the Director of National Intelligence. That process includes an interagency review of sensitive policy equities.

Do you see a need for a change in the decision-making process?

I believe that the recent improvements to the policy review process described in PPD-28 should be sufficient to ensure that all US government and privacy interests are considered prior to engaging in cyberspace operations. I have no specific recommendations for additional changes at this time.

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, that could be comparable to those caused by weapons of mass destruction.

Under what circumstances, if any, would you as Commander, U.S. Cyber Command, have the authority to use offensive cyber weapons without prior approval by the President?

Under current policy, Commander, U.S. Cyber Command would not use cyber capabilities for offensive purposes without prior approval by the President.

Are U.S. Cyber Command forces the only forces permitted to conduct offensive military cyber operations?

The President or Secretary of Defense could authorize any Combatant Command to direct assigned cyber forces to conduct military cyberspace operations. At present, we are building a Cyber Mission Force, which will be able to conduct these operations under the command and control of whichever Combatant Command to which they are assigned.

Are there official rules barring non-CYBERCOM forces from, for example, causing cyber effects against battlefield weapons systems, as an extension of traditional electronic warfare capabilities?

As far as I am aware, there are none.

Are there clear distinctions between cyber warfare and electronic warfare?

While there are clear distinctions between electronic warfare and cyber warfare, there may also be avenues to achieve greater operational synergy between these two missions and to examine the policy implications of their synchronized use in warfare.

Laws of War

Has the Department of Defense 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 (terrorists, criminals), and both when the source of an attack is known and unknown?

Per DoD guidance, all military operations must be in compliance with the laws of armed conflict-this includes cyber operations. The law of war principles of military necessity, proportionality and distinction will apply when conducting cyber operations.

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

N/A

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 classified information or capabilities had been compromised. These choices are referred to as "balancing equities" or "gain-loss" calculations.

Who is in charge of the equities/gain-loss process for cyberspace within the military?

There is a clear framework established to adjudicate the equities/gain-loss and is part of both crisis and deliberate planning efforts on the part of the Combatant Commanders. The risk-loss equation in the DOD is made after comprehensive consultation with the intelligence community and the impacted Commander. U.S. Cyber Command is the lead for DOD cyberspace deconfliction and is directly involved in cases of disagreement as part of the processes directed in key interagency documents. If the inter-agency disagreement is not resolved at this level, the issue goes to the Chairman Joint Chiefs of Staff, the Secretary of Defense, NSC Deputies and later to the President where the issue is resolved.

If these decisions rest with the Commander of U.S. Cyber Command, how will the combatant commands, the military services, and other defense agencies be persuaded that their interests will be fairly balanced with those of NSA?

PPD-20 allows for representation from other agencies, giving each a voice in the process. When gain-loss issues arise, all parties have the responsibility to comprehensively state the issues and impacts with these discussions beginning at the action officer level. Formal disagreements unresolved after U.S. Cyber Command review follow a clear path to department and national decision makers, to include the President if need be.

Since NSA personnel are filling a large number of key positions within CYBERCOM, how can you be confident that equity issues make it to senior levels in CYBERCOM, and are fully and fairly examined?

The value of NSA's contribution to the CYBERCOM mission in terms of manpower and mission support is vitally important; however, I believe that the military and civilian personnel in the current USCYBERCOM workforce contains a broad mix of experience and background from across the defense, intelligence, operations and law enforcement communities. Within the intelligence directorate for example, the Defense Intelligence Agency is the primary provider of personnel, with a senior executive from that agency holding the deputy director position. Staffing the leadership from a wide range of sources is a strength that has resulted in a more diverse level of input into the equities process than ever before. All issues requiring senior

leadership attention are fully and fairly vetted through a rigorous system of boards and working groups, made up of representation from across our diverse leadership cadre.

How are equities/gain-loss decisions 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?

The Tri-lateral Memorandum of Agreement contains a deconfliction mechanism involving DOD, DoJ, the Intelligence community and agencies outlined in, and reinforced by PPD-20. Disagreements are handled similar to those internal to DOD; the issue is forwarded from the Seniors involved to the Deputies then on to the Principals Committee with the final stop being the President in cases where equities/gain-loss are ultimately resolved.

As a foreign intelligence agency, NSA has a mission to find vulnerabilities in the networks of our adversaries. However, the NSA's Information Assurance Directorate is responsible for securing national security systems and CYBERCOM has the responsibility of defending DOD networks and the Nation.

How do you believe these responsibilities should be balanced?

The basis for handling discovered vulnerabilities must be the national interests of the United States. Understanding particular vulnerabilities, and how they may impact our national interests, requires deep understanding of the technology, the risks a vulnerability can pose, options for mitigating these risks, and the potential for foreign intelligence if the vulnerability remains open. But the balance must be tipped toward mitigating any serious risks posed to the U.S. and allied networks. NSA has always employed this principle in the adjudication of vulnerability findings, and if confirmed, I intend to sustain the emphasis on risk mitigation and defense.

What are the policies and processes that apply to the discovery and disclosure of so-called "zero day" vulnerabilities in software?

Within NSA, there is a mature and efficient equities resolution process for handling "0-day" vulnerabilities discovered in any commercial product or system (not just software) utilized by the U.S. and its allies. The basis for it is documented in formal NSA policy, which includes the adjudication process. The policy and process ensure that all vulnerabilities discovered by NSA in the conduct of its lawful missions are documented, subject to full analysis, and acted upon promptly.

NSA is now working with the White House to put into place an interagency process for adjudication of 0-day vulnerabilities. If confirmed, I will support this process.

What is the impact of not disclosing these vulnerabilities? What is the impact of disclosing them?

When NSA discloses a vulnerability discovery to a vendor, the goal is to achieve the most

efficient and comprehensive mitigation of the risk. Upon disclosure, vendors usually fix the vulnerability, and issue an update or patch. The risk is mitigated only when users actually install the patch. Since adversaries frequently study industry patches to learn about underlying vulnerabilities that will remain in unpatched systems, NSA disclosure of a vulnerability may temporarily increase the risk to US systems, until the appropriate patches are installed.

When NSA decides to withhold a vulnerability for purposes of foreign intelligence, then the process of mitigating risks to US and allied systems is more complex. NSA will attempt to find other ways to mitigate the risks to national security systems and other US systems, working with stakeholders like CYBERCOM, DISA, DHS, and others, or by issuing guidance which mitigates the risk. If confirmed, I intend to strengthen collaboration with other government stakeholders, under the auspices of the planned interagency process.

What is the impact of not disclosing these vulnerabilities? What is the impact of disclosing them?

NSA currently follows its equity resolution process, as required under NSA policy. Technical experts document the vulnerability in full classified detail, options to mitigate the vulnerability, and a proposal for how to disclose it. The default is to disclose vulnerabilities in products and systems used by the U.S. and its allies. The information assurance and intelligence elements of NSA jointly participate in this process.

Deterrence and Escalation Control

Does the U.S. Government have a cyber warfare deterrence strategy or doctrine?

Deterrence in cyberspace is achieved through the totality of U.S. actions, including the United States overall defense posture and the resilience of our networks and systems. As the President stated in his *International Strategy for Cyberspace,* the United States reserves the right to defend itself against cyberattacks. Whenever possible, the United States will exhaust all options prior to military force, and will always act in accordance with US values and in a manner consistent with the Constitution and international law. This Administration has articulated these policies consistently since the *International Strategy for Cyberspace* was published in 2011.
The establishment of U.S. Cyber Command is an element of a deterrence strategy, but more work and planning will be required to evolve a solid national strategy.

Cyber warfare is a complex and evolving discipline, and the subject of deterrence is drawing increasing attention at all levels of government and the Interagency, and in our discussions with our international partners. If confirmed, I will work with DoD, DHS, DOJ/FBI and others as we work to establish the relationships and engagement necessary to build such a strategy and policy.

Would you agree that 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?

Classic deterrence theory is based on the concepts of threat and cost; either there is a fear of reprisal, or a belief that an attack is too hard or too expensive. Cyber warfare is still evolving and much work remains to establish agreed upon norms of behavior, thresholds for action, and other dynamics. A broad understanding of cyber capability, both defensive and offensive, along with an understanding of thresholds and intentions would seem to be logical elements of a deterrence strategy, both for our allies and our adversaries and as they are in other warfighting domains. I believe we'll see much discussion of the structure and implementation of our cyber deterrence strategy from DoD and Intelligence Community experts, along with Interagency engagement.

How do you reconcile the utility of speaking more openly and candidly about cyber warfare capabilities in the interest of promoting greater public knowledge and the development of deterrence doctrine with the continued need to classify U.S. cyber capabilities?

I believe that as we communicate more with the public, the understanding that the U. S. will defend and deter in cyberspace, in accordance with law and international agreement, is more important than understanding the intricacies of the capabilities it will use to do so. I believe the public will understand that we do not want to telegraph our strategy for action to the adversary. As cyberspace matures as a warfighting domain, I believe our classification policies will also evolve to support growing domestic and international partnerships and relationships. Regardless, we will adhere with all classification policies and practices dictated by Executive Order.

Most experts believe that the attacker has a substantial advantage over the defender in cyber warfare. It is also widely believed that 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.

What are your views of these dynamics?

There is no doubt that the dynamics of offense and defense in cyberspace are complex, simply due to the physics of the engagement space. Automated capabilities, human response cycles, and many other factors make them even more so. These considerations are discussed and debated by experts across the whole of government, industry, and academia on a near-constant basis. The science and the philosophy are evolving. Just as it took time for doctrine, strategy, and concepts of deterrence and escalation to evolve in the other warfighting domains, so it is with cyber warfare. I believe we are making progress.

Implications of U.S. Dependence on Cyber Networks

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.

How could the Department compensate for U.S. dependence on vulnerable cyber networks in developing effective deterrent strategies?

We have effective deterrent strategies in place in the other warfighting domains, in the form of our demonstrated military might and capability. Cyber deterrence should evolve in the same way; demonstrated capability to defend, respond or be able to attack when necessary is a key to deterrence. Our dependence on our networks can be compensated for by having a strong, viable defense in the form of both traditional military strength and cyber capability. We have the ability to respond proportionately and discriminately in both kinetic and non-kinetic modes when we can meet attribution requirements.

We need, however, to move from what is currently a reactive posture, to a proactive one. We are integrating and synchronizing our military operations and supporting intelligence capabilities for optimal detection, analysis, assessment, and response to mitigate threats and vulnerabilities on a near-real-time basis. The concepts we are maturing in the form of multi-layered approaches and scalability, in coordination with DHS and others, are expandable to the rest of our government and critical infrastructure.

Our networks are inherent to our way of life; their vulnerability is the key concern. A strong and deterrent defense, along with robust, resilient networks, will alleviate that vulnerability.

Given our vulnerabilities, is it in our interest to avoid engaging in certain kinds of offensive cyber warfare – so that we do not set precedents by example for others to follow?

Any decision to engage in offensive cyber operations must reflect careful consideration and due diligence of the range of potential impacts, including adversary responses and the impact upon norms and precedents in cyberspace. Even as we must be prepared to undertake offensive cyber operations, these are important considerations in the decision to undertake such operations.

<u>The Challenge of Attribution</u>

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 – the problem of "attribution."

Can deterrence be an effective strategy in the absence of reliable attribution?

Yes, I believe there can be effective levels of deterrence despite the challenges of attribution. Attribution has improved, but is still not timely in many circumstances. We must employ several approaches to this challenge. A healthy, engaged partnership with the Intelligence Community is vital to continued improvement in attribution. Second, is development of defensive options which do not require full attribution to meet the requirements of law and international agreement. Cyber presence, being forward deployed in cyberspace, and garnering the indications and warnings of our most likely adversaries can help (as we do with our forces dedicated to Defend the Nation). We must ensure we leverage the newest technology to identify our attackers before and during an attack – not just after. Last, and perhaps most important, we need to make our

networks and supporting architectures robust, resilient, and defensible by establishing and encouraging adherence to cybersecurity and information assurance standards. This last is a national problem across all of our networks, and is one which we should actively work to resolve.

There are other actions that need to be taken, too, in order to advance our defensive capability and support a deterrent posture. These include partnerships with nation-states who share common goals and expectations for behavior in cyberspace. From these partnerships, we can build normative standards, thresholds for action, and evidential frameworks on which to base response. We also need to improve our relationships with private and industrial sector partners through information sharing regarding threat and vulnerabilities.

I believe the U.S. may be considered an easier mark because our own processes and criteria for response lead the adversary to believe, rightly or wrongly, that we do not have the will to respond in a timely or proportionate manner, even when attribution is available. This is within our capacity to fix.

The bottom-line is that we have much we can do to increase our posture to prevent attacks, mitigate them to at least a reasonable extent, or deter them outright, without full attribution.

Can the attribution problem be solved without comprehensive information sharing among the private sector and with the government?

I believe that the difficulty of attribution is compounded without a close relationship with the private sector, and full information sharing to the degree that policy and law allow. Most of our national information systems and networks ride on or are composed of infrastructure that is privately owned; we need their engagement to build attribution capability.

<u>Systems Acquisition</u>

Combatant Commands by design play a limited role in the acquisition process. However, the Commander of U.S. Cyber Command is dual-hatted as the Director of the National Security Agency (NSA), which is a large enterprise with substantial resources for developing, procuring, and supporting new equipment, systems, and capabilities. In addition, the Commander exercises operational control of Defense Information Systems Agency (DISA) networks, and DISA is also an agency that acquires systems and capabilities.

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?

If confirmed as the Commander, USCYBERCOM, I will rely upon the acquisition authority of other organizations, (e.g., the Services and Defense Agencies) to equip the cyber forces to satisfy validated operational requirements and comply with DoD policy and capability development guidance. This is the same process used by the other Combatant and Sub-Unified Commands,

with the exception of U.S. Special Operations Command.

What measures have been taken to ensure 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 U.S. Cyber Command without the rigor required by the DOD requirements and acquisition processes?

USCYBERCOM, NSA and DISA are all separate organizations with their own, ability to acquire personnel and equipment, processes and staffs. Due to the separate nature of these three organizations, the oversight, accountability chains, and the ability to audit will ensure I follow the USCYBERCOM requirements process and the Director of NSA follows the established NSA acquisition process. And as mentioned earlier, USCYBERCOM will operate under the same authorities and oversight as other Combatant Commands and Sub-Unified Commands.

Specifically regarding rigor, USCYBERCOM adheres to all laws and policies regarding acquisition and if confirmed, I will ensure DOD requirements and acquisition processes will continue to be followed.

Specifically, I understand the Department directed USCYBERCOM to establish the DoD Cyber Operational Capabilities Board (COCB) to better integrate military cyber capabilities requirements into cyber capability development. The COCB is in its infancy and the DRAFT Charter is still being staffed, but it will be fully alignment with the Department's Joint Capabilities Integration and Development System (JCIDS) to ensure future cyberspace capability development supports the Combatant Commands.

It is important to note that although USCYBERCOM, as a sub-unified command, does not have its own acquisition authority, it has the management controls necessary to ensure Command activities for funding capability developments satisfy validated operational requirements and comply with DOD policy and capability development guidance. While USCYBERCOM does not have the acquisition authority to designate a Milestone Decision Authority (MDA), the Command makes investment decisions that result in starting, continuing, suspending, or terminating its investments in cyberspace capability developments. These decisions are made in concert with executing MDAs and reflect the Command's focus on funding only those capability developments that will deliver required operational cyberspace capabilities within the timeframes needed. As discussed previously, USCYBERCOM will rely upon the acquisition authority of other organizations, e.g., the Services and Defense Agencies.

The National Defense Authorization Act for Fiscal Year 2011 required the Secretary of Defense to establish a strategy for streamlining the acquisition and oversight process for cyber warfare capabilities, which resulted, among other things, in the establishment of the Cyber Investment Management Board (CIMB).

Three years after the passage of this legislation, how would you characterize DOD's progress in establishing an agile acquisition process to provide capabilities for U.S. Cyber Command?

The CIMB was established in 2012 and has been meeting on a quarterly basis. The CIMB is chartered to provide strategic guidance and recommendations to support integration and synchronization of cyber capabilities across science and technology requirements, acquisitions, development, test and evaluation, and sustainment to ensure that cyber warfare investments are efficiently planned, executed, and coordinated across the Department. The CIMB continues to mature and is working to demonstrate a streamlined acquisition and oversight process for cyber warfare capabilities. Currently, they have identified pilot programs to demonstrate the proof of principle for rapid acquisition of cyber capabilities.

Military Service Roles in U.S. Cyber Command

Each of the military services is producing cyber operations units for assignment to U.S. Cyber Command to defend the nation, support the other combatant commands, and to defend DOD networks.

Are these Army, Navy, Marine Corps, and Air Force units geographically organized and assigned, or is there also specialization among the military services by mission or type of target?

Service provided Cyber Mission Force Teams are both geographically aligned and specialized depending upon their assigned mission area.

The Cyber National Mission Force is comprised of National Mission Teams, National Support Teams, and National Cyber Protection Teams. They are assigned to the "Defend the Nation" in cyberspace mission area and, if directed, defend our critical infrastructure and key resources (CIKR) against Nation State and Non-State actors.

The Combat Mission Forces are comprised of Combat Mission Teams and Combat Support Teams. They are assigned to the "Provide Support to Combatant Commands" mission area. Combat Mission Forces are geographically and functionally aligned under one of four Joint Force Headquarters-Cyber in direct support of geographic and functional combatant commands. They are aligned as follows:

- JFHQ-C Washington supports U.S. Special Operations Command, U. S. Pacific Command, and U.S. Southern Command
- JFHQ-C Georgia supports U. S. Central Command, U. S. Africa Command, and U. S. Northern Command
- JFHQ-C Texas supports U. S. European Command, U. S. Strategic Command, and U. S. Transportation Command

The Combat Protection Forces are comprised of Service, Defense Information Systems Agency, and Combatant Command Cyber Protection Teams. They are assigned to the "Secure, Operate and Defend the Department of Defense Information Networks (DODIN)" mission area. These teams are specialized to prepare and protect key cyber terrain to provide mission assurance.

Would, for example, Army units be assigned to operate against naval or air targets, and vice versa?

Yes, targets developed for fires and effects delivered in and through cyberspace do not necessarily correspond with traditional Service domains much as an Air Force unit may we be tasked to attack a naval vessel. The cyberspace domain often intersects with multiple elements of a single target. A Target System Analysis that yields multiple aimpoints provides a commander flexibility on how best to prosecute the target with the least risk. These options may require an Army unit to operate against naval or air targets and vice versa. Ultimately, the Joint Force Commander will determine how best to engage a target with the cyber mission forces at his/her disposal.

Will each geographic combatant command have a mix of units from each military service?

Each geographic combatant command is supported by a Joint Force Headquarters-Cyber with personnel from all Services, and with the exception of U. S. Africa Command, all GCCs have a combination of Service established Cyber Mission Force teams aligned. Currently, all U. S. Africa Command Cyber Mission Forces are U. S. Army provisioned.

Will geographic combatant commanders be permitted to execute cyber operations under their own authorities?

Geographic combatant commanders already have authority to direct and execute certain Defensive Cyberspace Operations (DCO) within their own networks. These actions consist of internal defensive measures to prepare and protect mission critical networks. In the event of hostilities or contingency operations, Combatant Commanders would be permitted to execute full spectrum cyber operations as approved by the President and directed by the SECDEF.

<u>Focus on Intelligence Gathering versus Focus on Warfighting</u>

The National Security Agency (NSA), as an intelligence agency, appropriately places the highest importance on remaining undetected, and accordingly invests in high-end – and therefore expensive and hard-to-develop – technical tools and tradecraft, following a deliberate methodology for developing and maintaining capability. U.S. Cyber Command (CYBERCOM), as a military combatant command, has very different interests and objectives. For example, it must have the capability to act rapidly, it may need tools and processes that do not require computer scientists to operate them, and it may need to act in a fashion that makes it clear that the operation is an attack by the United States.

Do you believe that you could direct CYBERCOM wartime operations effectively if CYBERCOM were only able to use the NSA infrastructure to support those operations?

It depends. We must ensure we have the tools and infrastructure needed to accomplish our

mission whenever necessary. USCYBERCOM should leverage the NSA platform where appropriate and cost-effective, while developing additional infrastructure to accomplish military operations that are unique and distinguishable from the intelligence community.

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

NSA's infrastructure and tools could be scaled to support combat operations in cyberspace. To most effectively manage risks across military and intelligence operations in cyberspace, USCYBERCOM and the Services need to leverage NSA expertise to build cyberspace capabilities for combat operations which could include additional tools and infrastructure that are unique and distinguishable from the intelligence community.

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

As the Services field Cyber Mission Forces (CMF) in accordance with Joint Staff guidance, capability development should occur concurrently to ensure the CMF have the requisite facilities, platform, equipment, and tools needed to accomplish their assigned mission. In many cases, Cyber forces, to be operationally effective, would need to retain the capability to operate in a manner which conceals the detailed specifics of U.S. military capabilities. If we were to operate "in the clear," we may expose our tradecraft, tools and infrastructure. If we do that, our enemy can deny us our capability and, in some cases, replicate it and use it against us.

Section 932 of the National Defense Authorization Act (NDAA) for Fiscal Year 2014 requires the Secretary of Defense to provide CYBERCOM with infrastructure to enable CYBERCOM to independently access global networks to conduct military operations.

What are your views on this requirement?

There is no doubt that collocating CYBERCOM with NSA, and dual-hatting the Commander and Director, allows for efficient use of available platform capabilities and technical expertise. I do believe; however, that CYBERCOM needs additional infrastructure to accomplish military operations that are unique and distinguishable from the intelligence community. The Department has made significant progress recently in identifying and planning for development of alternative, diverse, scalable, deployable, and disposable platforms that can be available on demand to the Cyber Mission Force for mission accomplishment.

What is your understanding of the Department's plan for complying with the legislation?

My understanding is that CYBERCOM has already been tasked by the Deputy Secretary of Defense and has made measurable progress in laying out a strategy for identifying the numbers and mix of alternative platforms required to meet operational requirements, both for steady state and contingency purposes. These platforms will give the Cyber Mission Force the diversity and scalability needed to address the threat, apart from the intelligence platform. Additionally, since

they do not require the breadth and sophistication of the existing platform, they should be less expensive to build and deploy.

Do you believe DOD can implement the legislative direction in an effective and affordable manner?

Yes, there has been a significant amount of effort expended by the Department toward meeting this requirement.

Development of Cyber Officer Corps

In a forthcoming article, the J3 of CYBERCOM, Major General Brett Williams, argues that: "*We have a pressing need to develop cyberspace operators who are credible and effective in the J3 and J5, within both the Joint Staff (JS) and the Combatant Commands (CCMD).* Just for emphasis, that is the J3 and J5, not just the J2 and J6; and at all of the CCMDs, not just CYBERCOM…Joint staffs consist of what we typically think of as operators, members of the combat arms who are educated, trained and experienced in operations. Cyberspace expertise usually comes from people with intelligence, communications or cryptology backgrounds; career fields typically categorized as support forces. If we are going to treat operations in cyberspace like operations in the other domains, the services must commit to unique career fields for cyberspace… Cyberspace, like the other domains, requires officers who are developed across their careers in a way that positions them to lead at senior levels in both command and staff. Cyberspace officers should spend their first ten years becoming tactically proficient in all aspects of cyberspace operations, complete service and joint military education, serve on joint staffs, command in their area of operational specialty and do all of the other things necessary to produce General and Flag officers whose native domain is cyberspace."

What are your views about whether cyber officer career development should be distinct from both intelligence and communications officer development?

Specialized expertise in our officer ranks is critical to mission accomplishment. At the same time, a shared understanding across the team is essential. The way we have deliberately approached this in the Navy has been the establishment of Cyber Warrant Officers and Cyber Warfare Engineers. These individuals are purposefully selected to join our ranks from either our enlisted force, the intelligence community, academia, or industry. We then train and employ them to leverage their specialized expertise. They serve side by side with Officers from varied career fields, but primarily intelligence and communications specialists although combat arms officers could be trained as cyber officers as well. I believe all officers should have an appreciation for cyberspace operations. Intelligence and communication officers must have a clear understanding of the same, and we have a responsibility to develop specialized expertise in a core of cyber officers.

Is it advisable to develop cyberspace officers as we do other combat arms or line officers? Why or why not?

I am a strong proponent of diversity across the team and quick to recognize all have a responsibility to both understand and contribute in this mission area. We must find a way to simultaneously ensure combat arms and line officers are better prepared to contribute, and cyberspace officers are able to enjoy a long, meaningful career with upward mobility. A meaningful career should allow them to fully develop as specialized experts, mentor those around them, and truly influence how we ought to train and fight in this mission space. I am especially interested in the merit of how a visible commitment to valuing cyberspace officers in our ranks will affect recruitment and retention. I believe that many of today's youth who are uniquely prepared to contribute (e.g. formally educated or self-developed technical expertise) do not feel there is a place for them in our uniformed services. We must find a way to strengthen the message of opportunity and I believe part of the answer is to do our part to ensure cyberspace officers are viewed as equals in the eyes of line and combat arms officers; not enablers, but equals. Equals with capabilities no less valued than those delivered by professional aviators, special operators, infantry, or surface warfare.

Alignment of Military Cyber Operations with Cyber Intelligence Collection

Do you think that, as CYBERCOM matures and as cyber military art develops, military cyber operations and cyber intelligence operations should be distinct operations?

Intelligence is a joint function integral to all military operations. Intelligence operations are conducted in cyberspace to inform military operations in all domains, including cyberspace.

In the long term, what are the pros and cons of treating the services' cyber organizations and the service cryptologic elements as distinct entities?

Just as there is a dynamic partnership between U.S. CYBERCOM and NSA, and the disciplines of military cyber operations and cyber intelligence operations are interwoven, there is a similar relationship and advantage to be had in the partnerships between the service cryptologic and cyber organizations. They provide key capability to their services as independent focal points for warfighting and intelligence, but together provide the additive cyber capability for each service. If confirmed, I will continue to assess the cyber force model as it develops in view of this synergism.

Do you think that military cyber operations personnel assigned to CYBERCOM units should, in the long term, continue to be funded mainly in the intelligence budget and competing with intelligence priorities?

In view of our current fiscal environment and challenges, if confirmed, I would examine and assess all CYBERCOM funding streams and processes, including personnel.

Range Support for U.S. Cyber Command

Section 932 of the National Defense Authorization Act (NDAA) for Fiscal Year 2014 requires the Secretary of Defense to ensure that there are adequate range capabilities for training and exercising offensive cyber forces in operations that are very different from cyber intelligence operations.

What is your understanding of CYBERCOM's range requirements for individual and unit training, and exercises, and the capabilities and capacity of the joint cyber range infrastructure to satisfy those requirements?

It is my understanding that the persistent training and test environment is being developed based on requirements from USCYBERCOM's exercise continuum of CYBER KNIGHT, CYBER GUARD, and CYBER FLAG. This continuum is designed to train and/or certify Cyber Mission Force teams. Unfortunately, these exercises are executed using not only ad hoc range support, but also ad hoc facilities. Though the lack of a range continues to be a limiting factor, so does the lack of a physical infrastructure. Though the main effort in building the teams is individual training and qualification right now, collective training and certification will quickly make the lack of efficient range even more glaring than it is today. Our cyber forces need a persistent training environment they can depend on every day of the week to train. We must continually train against a high end adversary and not only in CJCS level exercises. The key to success here is training. A persistent range is a must have if we want to build a professional cyber force.

What is your view of the NDAA legislation?

The Department continues to fully realize the potential of the DoD Enterprise Cyber Range Environment (DECRE) governance body to oversee Cyber Range issues. The main effort of DECRE is the establishment of a persistent test and training environment that will effectively meet the growing demand of the Cyber Mission Force teams. It is essential that we provide these teams, which are quickly reaching IOC and FOC in greater numbers, by providing on-demand environments for training in both offensive and defensive cyberspace operations. It is my understanding that the Department is on pace to deliver an assessment of the required cyber range capacity and capability to support Cyber Mission Force training by October 2014.

Information Assurance

The President's Review Group on Intelligence and Communications Technologies recommended that the Information Assurance Directorate (IAD) of the National Security Agency (NSA) be separated from NSA and subordinated to the cyber policy component of the Department of Defense. The Senate version of the National Defense Authorization Act for Fiscal Year 2014 included a provision that would transfer supervision of the IAD from the Under Secretary of Defense for Intelligence (USD(I)) to the Chief Information Officer (CIO). The Committee's rationale for this transfer was that the IAD conducts cyber protection-related duties, which fall under the responsibility of the CIO, not the USD(I).

What do you see as the pros and cons of these proposals?

I support the President's decision for the Information Assurance Directorate (IAD) to remain part of NSA. NSA has developed (and continues to develop) an extremely deep cadre of computer scientists, mathematicians, software engineers, etc. whose skills are translatable across the breadth of the Information Assurance (IA) and Signals Intelligence (SIGINT) missions. IAD and the Signals Intelligence Directorate (SID) operate in a common trade space, the global telecommunications network. NSA offensive and defensive missions have a proven track record of success at working together to counter the cyber threat. Code making and code breaking are two sides of the same coin. Breaking them apart will have significant consequences to the U.S. government's ability to develop secure communications based on the understanding of how those communications might be attacked.

NSA has developed an infrastructure that supports both Information Assurance and SIGINT missions. Creating a separate agency that would need to develop and build its own infrastructure and expertise would be extremely inefficient and costly in a time of constrained resources. IAD guidance and technology helps secure the NSA enterprise. The work IAD performs benefits the security of the nation and the world. Current Media Leaks have unfortunately caused degradation in our trust relationships with industry. If confirmed, I am committed to restore the trust and will deepen the partnerships with the DoD CIO and the USD(I) to demonstrate oversight procedures and processes function appropriately.

Dual Hatting of Director of the National Security Agency and the Commander, U.S. Cyber Command

The President's Review Group on Intelligence and Communications Technologies recommended that the positions of Director of NSA and the Commander of CYBERCOM be separated and that the President appoint a civilian to be Director of NSA. The President decided against separating these two positions at this time. According to press reports, the President based his decision, in part, on his perception that CYBERCOM was not yet mature enough to stand on its own without a very strong institutional connection to NSA.

If CYBERCOM remains too dependent on NSA for their leadership to be bifurcated, does it follow that CYBERCOM is not mature enough to become a full unified command?

My focus on sub-unified or unified will rest on what allows USCYBERCOM to achieve the most effective cyber force – one that is best postured to defend the nation and our national interests.

The decision by Secretary of Defense to re-designate the position of Director, NSA as both Commander, USCYBERCOM and Director, NSA enabled DoD to leverage the similarities and overlaps between the capabilities needed for the conduct of NSA's core missions – Signals Intelligence (SIGINT) and Information Assurance (IA) – and those of USCYBERCOM to provide for the defense and secure operation of DoD networks; and, upon order by appropriate authority, to operate in cyberspace to defend the nation. The strength of this arrangement as the

most effective approach to accomplishing both organizations' missions was re-affirmed with the President's December 2013 decision to retain the dual-hat position.

To the extent that military operations in cyberspace should evolve to be different and distinct from intelligence collection in cyberspace, is it possible that NSA's strong influence over CYBERCOM's development could hinder, as well as support, the proper maturation of the Command? What are your views on this issue?

I will ensure NSA, as a combat support agency, continues to support USCYBERCOM's ability to execute its mission as well as its maturation. For example, there is a high correlation between the knowledge, tools, and techniques necessary for meeting military objectives and those for enabling intelligence collection. This correlation allows economy of scale in tool and technique development. In addition, I will ensure that USCYBERCOM has control over the assets it needs and I will work within DoD to ensure USCYBERCOM has the support it needs to be successful. As the dual-hatted Director/Commander, I will empower the Deputy Director, NSA and Deputy Commander, USCYBERCOM to focus on running their respective organization with mission equities in mind, while I maintain accountability with insight into both missions and direct collaboration when necessary.

As NSA is a combat support defense agency subject to the authority, direction, and control of the Secretary of Defense, and NSA is subordinate to the Secretary of Defense in his capacity as the President's executive agent for signals intelligence under Executive Order 12333, is there any reason to expect that NSA's support for CYBERCOM and the other combatant commands would be questionable if the dual-hat arrangement were ended?

NSA has a long history of supporting combatant commands with SIGINT and Information Assurance (IA) products and services, well before USCYBERCOM was established. I will ensure NSA provides mission critical support to all combatant commands, with or without the dual-hat arrangement.

U.S. Cyber Command as a Sub-unified Command

The Unified Command Plan (UCP) establishes U.S. Cyber Command as a sub-unified command reporting to U.S. Strategic Command. We understand that the Administration considered modifying the UCP to establish U.S. Cyber Command as a full combatant command.

What are the best arguments for and against taking such action now?

I understand that there was discussion at the CJCS and Service Chiefs' level in 2012 to establish U. S. CYBERCOM as a full unified command, and that discussion of this option has continued.

I don't believe there are any major impediments to elevating U. S. CYBERCOM to full unified command status, with the exception of adding approximately 112 personnel to our headquarters manning (currently 912) required to accomplish administrative functions that would accompany unified command

status, such as workforce recruitment, Planning, Programming, Budgeting and Execution (PPBE); and Global Force Management. In addition, there are formal processes that would have to be executed, including revision to the current Unified Command Plan language, but cyberspace operations comprise both a warfighting and enabling discipline and domain in and of itself. Cybercom is working incredibly hard every day to develop its forces, processes, and capability, so perhaps the best argument against elevating the command is the need to focus energies in these areas.

The argument for full Unified Command status is probably best stated in terms of the threat. Cyber attacks may occur with little warning, and more than likely will allow only minutes to seconds to mount a defensive action seeking to prevent or deflect potentially significant harm to U.S critical infrastructure. Existing department processes and procedures for seeking authorities to act in response to such emergency actions are limited to Unified Combatant Commanders. If confirmed, as the Commander of U.S. CYBERCOM, as a Sub-unified Combatant Commander I would be required to coordinate and communicate through Commander, U.S. Strategic Command to seek Secretary of Defense or even Presidential approval to defend the nation in cyberspace. In a response cycle of seconds to minutes, this could come with a severe cost and could even obviate any meaningful action. As required in the current Standing Rules of Engagement, as a Combatant Commander, I would have the requisite authorities to directly engage with SECDEF or POTUS as necessary to defend the nation.

There are some inherent inefficiencies in not elevating, also, in the form of redundant processes and timeliness. Elevation to full unified status would improve resource advocacy, allocation and execution by improving input to Department processes and eliminating competition in prioritization. Additionally, alignment of responsibility, authority, situational awareness, and capability under a single commander would improve cyberspace operations and planning.

What authorities for operating in cyberspace that are allocated to STRATCOM have been pre-delegated to CYBERCOM?

USCYBERCOM has been delegated by CDRSTRATCOM the responsibility to conduct specified cyberspace missions as detailed in Section 18(d)(3) of the Unified Command Plan. The specific missions delegated include: directing DODIN operations, securing and defending the DODIN; maintaining freedom of maneuver in cyberspace; executing full-spectrum military cyberspace operations; providing shared situational awareness of cyberspace operations, including indications and warning; integrating and synchronizing of cyberspace operations with combatant commands and other appropriate U.S. Government agencies tasked with defending the our nation's interests in cyberspace; provide support to civil authorities and international partners.

<u>Support for the Combatant Commands</u>

The Secretary of Defense has ordered the military services and CYBERCOM to develop operational military cyber teams to support the missions of defending the nation against cyber attacks, supporting the war plans of the geographic and functional combatant commands, and defending Department of Defense networks against attacks.

The mission teams that will support the combatant commanders ultimately will be under the operational control of those commanders. The Committee understands that, to date, the combatant commands have not committed to creating cyber component commands to direct the operations of those units.

In your opinion, can the combatant commanders properly direct the operations of assigned cyber mission teams without a component command element?

Geographic combatant commanders already have the authority to direct and execute certain Defensive Cyberspace Operations (DCO) within their own networks. These actions consist of internal defensive measures (DCO-IDM) to prepare and protect mission critical networks. The current Joint Staff C2 model provides an interim construct to direct DCO-IDM through a Joint Cyber Center/Cyber Support Element. Combatant commanders direct full-spectrum Cyberspace operations (ISR, OPE, Attack and Defend) through a Joint Cyberspace Component Command to ensure actions are synchronized and integrated throughout all warfighting domains. A JFCCC also provides for accountability through legal oversight and compliance – a requirement for Cyberspace Operations. Until a JFCCC is establish, a Joint Force Headquarters directly supports combatant command planning, execution and oversight.

Four years after the creation of CYBERCOM, to what extent have cyber operations been integrated into the operations plans of the combatant commands?

My understanding is that progress has been made in integrating cyberspace capabilities into the operations plans of the combatant commands. Although much work remains, USCYBERCOM has been successful in this effort by coordinating and cooperating with the combatant commands directly, by integrating cyberspace capabilities when the plans are undergoing Department-wide review, and also by drafting cyberspace support plans that supplement the higher level combatant command plans.

Additionally, CYBERCOM is building 27 cyber mission force teams assigned to the Combatant Commands to achieve exactly this kind of capability.

How would you assess the progress of the Department in developing cyber capabilities for the use of the command cyber teams to support the specific needs of the combatant commands?

The Services have made progress developing capabilities to equip their Cyber Mission Force (CMF) teams. At the Department's direction, USCYBERCOM has established, and now chairs, the DoD Cyber Operational Capabilities Board (COCB) which will integrate military cyber capability development into existing requirements processes.

In accordance with Department direction, USCYBERCOM has also begun implementing changes to the Cyber Capabilities Registry (CCR). The CCR is now populated and accessible, providing military planners a compendium of available cyberspace capabilities for use in support of mission requirements. Ultimately, the CCR will become an informative source for all DoD cyberspace capabilities.

USCYBERCOM recognized that we needed to make progress faster in developing the tools our warfighters need in cyberspace. As such we stood up a J9 inside the command and staffed it with the best and most qualified military and NSA personnel (lead by a NSA senior and US Army Colonel both with PhDs) to work with the services, industry, academia, the IC and our DoD labs to bring new ideas and tools to our cyber forces in the shortest time possible. This effort is starting to bear fruit delivering cyber tools our warfighters are already training with and integrating in tactical training exercise.

While the Department has made progress in this area, there is still much work to be done to ensure we develop joint, interoperable cyberspace capabilities to equip the Cyber Mission Forces as they become operational.

What priority has been assigned to the development of capabilities for national versus command cyber mission teams?

The prioritization of capability development for national and combatant command cyber mission forces flows directly from USCYBERCOM's three mission areas; (1) defend the nation; (2) secure, operate, and defend Department of Defense information networks (DoDIN); and (3) provide support to combatant commands. USCYBERCOM's highest priority is to defend the nation. This is done in parallel with activities dedicated to securing the DoDIN and supporting combatant commands. We are building out a robust cyber force over the next three years. While we rightfully have first focused on the DTN mission, we have simultaneously begun the buildout and IOC of our Combatant Command CMTs and CPTs. All of these mission areas are resourced in a balanced way in accordance with a continuous threat assessment and fiscal limitations.

Who would you say is responsible for developing cyber capabilities to support joint task forces and lower echelons?

The Services are responsible for developing capabilities to equip their forces. That said, USCYBERCOM plays a role coordinating operational and technical requirements to ensure interoperability for Cyber Mission Forces and compatibility with mission infrastructures. The DoD Cyber Operational Capabilities Board (COCB) provides a venue for much of the coordination to standardize military cyber capability development and leverage existing programs to avoid duplication of effort across the DoD. In its unique position, USCYBERCOM can and should form a community of operational and technical subject matter experts from across DOD and the IC to inform policy and resourcing decisions.

Development of Cyber Capabilities

CYBERCOM has depended heavily to date on NSA for technology, equipment, capabilities, concepts of operations, and tactics, techniques, and procedures.

Are you satisfied that the Department of Defense is organized and resourced to provide a broad base of innovation and capability development in the cyber domain that includes the

military service's research and development organizations, defense agencies such as the Defense Advanced Research Projects Agency, and the private sector?

While the Department has made much progress, more work certainly remains to ensure that DoD is organized and resourced to provide military-specific cyber capabilities. However, I believe the Department is moving in the right direction through a series of decisions to prevent redundancy and to ensure cyber innovation in both the public and private sectors can be leveraged. One of these decisions was to establish the aforementioned COCB to identify and track dependencies among capability requirements and to validate and prioritize all cyberspace capability requirements.

USCYBERCOM's Advanced Capabilities Directorate, J9 has existing relationships with the Services and their dedicated research and development labs, DARPA, federally-funded research and development centers (FFRDCs), the defense industrial base, the private sector, and other entities, allowing USCYBERCOM to leverage their expertise to provide and build diverse capability to enable full-spectrum military operations. As a member of the COCB, the J9 also helps enforce a process to ensure there is no redundancy of effort, and that several DoD entities can use the same capability multiple times when possible to get more return on investment.

Delegation of Signals Intelligence Authorities

How important will it be for CYBERCOM personnel to be able to operate with signals intelligence authorities that are not necessarily tied to National Security Agency personnel who may be working temporarily for CYBERCOM?

The ability of USCYBERCOM personnel to operate under delegated SIGINT authorities and leverage the national cryptologic platform is a critical capability, enabling the Command to fully execute its cyberspace mission in an informed, timely, and coordinated manner. Signals intelligence information remains vital to support cyber operations. Effective "net-speed" operations as conducted by an expanded U.S. cyber mission force require ready access to the technical streams of information that signals intelligence provides. Providing signals intelligence information at the lowest possible level in a distributed force environment makes the delegation effort especially important. Time delay increases the potential for mission failure. It is important to note that under delegated signals intelligence authorities, USCYBERCOM personnel adhere to the same uniform techniques, training and standards, as well as intelligence oversight and compliance programs, as those who work for the National Security Agency. We will not sacrifice our legal and security obligations to accomplish these goals.

Joint Information Environment (JIE)

The Defense Information Systems Agency (DISA) advertises the Joint Information Environment (JIE) programs as delivering:

". . . the largest restructuring of information technology (IT) management in the history of the DOD. The end state is a secure, joint information environment comprised of shared IT

infrastructure, enterprise services, and a single security architecture. JIE will enable DOD to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies."

To realize this potential, the CYBERCOM will have to operate within the JIE.

Has CYBERCOM developed plans for integrating its warfighting operations into the JIE?

In the JIE Management Construct (approved at the TANK), USCYBERCOM is responsible for identifying requirements and concepts of operation which enable and align with the Command and Control (C2) and defense of the DoDIN. JIE is a framework for which standards are being designed and built to meet these specified operational requirements.

Will the JIE systems architecture support a full range of potential CYBERCOM warfighting operations?

The JIE systems architecture supports the full range of operations 'of' and 'on' the DoDIN. The JIE will shift focus from protection of military service-specific networks, systems, and applications to securing data and its uses; a paradigm shift from the traditional net-centric to a data-centric environment. Key security features that will be employed under the JIE framework include: an enterprise-wide Single Security Architecture (SSA), a secure Out-of-Band (OOB) Management network; standardized identity and access management (IdAM); and the integration of thin-client and cloud-based (virtualization) technologies.

JIE changes the way the Department delivers IT capabilities in the largest, most complex operational environment in the world. Common services and capability will provide users information at the point of need from any networked device and from the enterprise level for all users. The ultimate beneficiary of the JIE will be the commander in the field and forces at the tactical edge. JIE will allow better integration of information technologies, operations, and cyber security at a tempo that supports today's fast-paced operational conditions. The operational capabilities delivered through the JIE will enable commanders to blend the art of command with the science of control, enabling JF 2020 to address emerging military challenges through the flexible integration of warfighting functions as required.

JIE will afford organizations responsible for operating and defending this complex environment end-to-end visibility and situational awareness for security from strategic to tactical as well as down to the desktop. It will eliminate the barriers which prevent information sharing and consolidate computing power and storage capabilities while enabling support for low-bandwidth/disadvantaged users.

Should DOD approach the JIE as more of a "weapons system" than a pure IT system in order to support the range of CYBERCOM's warfighting plans?

JIE is not a system, but is a framework of standards which the DoD Services and Agencies are using to procure, operate and defend the DODIN. JIE is focused on helping the DoD achieve full spectrum superiority, improved mission operational effectiveness and increased security

while realizing IT efficiencies. The JIE focuses on creation of a secured joint environment, comprised of a shared Information Technology infrastructure that will deliver common services from the enterprise, bound and secured by a single security architecture. The environment will be operated in accordance with responsibilities and authorities identified in the Unified Command Plan based on common, enforceable standards and specifications, as well as common Tactics, Techniques, and Procedures. The primary objective of creating the JIE is to provide DoD and mission partners secure access to Department IT capabilities at the point of need; i.e., home, work or deployed; by creating a Joint Enterprise Information Environment that encapsulates computing power; common enterprise services and mission applications; and access to data anywhere in the enterprise with the ability to extend the same capabilities in the deployed environment. However, once we build the underlying architecture(s) within the JIE framework, we need to look at them as a weapons system: measure its readiness, garner mission assurance, produce trained and ready operators, etc.

Security of Navy Networks

The *Wall Street Journal* last September reported that Iran had compromised the Navy Marine Corps Intranet (NMCI), an unclassified but important and pervasive internal communications network. The Navy has made an award for the successor to NMCI, called the Next Generation Enterprise Network (NGEN). The winning contractor is the same company that bought the original contractor for NMCI.

Is the NMCI properly architected and constructed against external cyber attacks? If not, why not?

Yes, NMCI is properly architected and constructed against external cyber attacks. Since its inception the NMCI architecture has evolved to respond to the threat environment. The threat environment has clearly changed and cyber security improvements have been made to NMCI over the years. The Navy and DoD defense in depth cyber security architecture, when combined with NMCI security layers, provide appropriate protection. As with all networks, the NMCI security architecture continues to mature as technology and threats evolve. Based upon operations over the last eight months and in collaboration with NSA, USCC, and DISA, I have identified additional network hardening and cyber security requirements for current and future Navy Networks that are currently being planned and programmed for implementation.

Is the NGEN architecture more secure than NMCI, and if so, in what respects?

Yes, NGEN benefits from lessons learned and technological advances but is designed on the same solid security principles used to develop NMCI. Its increased security will be the byproduct of three important factors: increased Navy Command and Control (C2) of a network the Navy "bought back" as a result of the transition from a Contractor Owned/Contractor Operated (CO/CO) model to a Government Owned/Contractor Operated (GO/CO) model; an increase in the Navy's ability to make and implement critical decisions about the selection of enterprise services under a more agile and innovative contract; and a firm commitment to align those services with the higher level Joint Information Environment (JIE) and Intelligence Community

(IC) Information Technology Enterprise (ITE). The NGEN contract also allows us to add, modify, and delete services in addition to lowering overall operating costs through competition.

Is the NGEN program fully aligned with the security architecture of the Joint Information Environment (JIE) initiative? If not, why not?

Yes, NGEN is designed and architected to current security standards and will leverage Technical Refresh and additional security funding to align to the JIE Single Security Architecture (SSA) as it becomes better defined, documented, and tested. Navy is participating actively in DoD's drive to define the SSA and the other components that will come together to form JIE. It has been playing a particularly active and important role in defining how the emerging SSA and related components will apply to JIE Increment II, which will properly secure U.S. and multinational information flows under the transformational Mission Partner Environment (MPE). As the definitions take shape, Navy will take decisive action to bring NGEN into alignment with JIE's SSA.

What steps and how much time and investment will it take to align NGEN with JIE?

The DoN supports the concept of JIE and is working in coordination with the other Services, DISA, COCOMs, and OSD to fully develop this concept into a joint enterprise capability. By continuing such engagement, Navy will develop better insights regarding the time and money required to bring its NGEN into alignment with these higher-level architectures. At present, we are of the belief that our agile and innovative contracts and the investments we've already programmed across the FYDP within NGEN and our other IT infrastructure and network programs (e.g., Consolidated Afloat Networks and Enterprise Services (CANES) and OCONUS Navy Enterprise Network (ONE-Net)) constitutes a sufficient response to the challenge at hand. As the standards for JIE mature, Navy will be able to provide cost and schedule estimates using NGEN as our path to meet JIE standards.

Cyber Personnel

What is your understanding of the direction DOD has given to the military services regarding the quality and existing skill levels of the personnel they will provide for the cyber mission forces?

On behalf of the DOD (IAW CJCSI 3500.01G), USCYBERCOM establishes Cyber Mission Forces joint standards for individual and collective training. These standards are contained in three foundational documents; the Joint Cyberspace Training and Certification Standard (JCT&CS), the Individual Training Pipelines, and the Training and Readiness Manual (T&R Manual). The JCT&CS identifies the unique Knowledge Skills and Abilities (KSAs) for each work role on the CMF Teams. The individual training pipelines outline an optimal path to achieving the required KSAs to satisfy the JCT&CS requirements. The T&R Manual provides the tasks, conditions and standards required to demonstrate individual and collective proficiency.

So far, does it appear that there is a satisfactory match between the skills and aptitudes of the personnel provided by the services and the training programs developed by CYBERCOM?

The Cyber Mission Force build out, when complete, will include over 6,100 personnel organized across 133 teams in the Cyber Mission Forces. As we build this force, work roles have unique training requirements and we must continue to create sustainable, repeatable training programs to meet this demand. Over the past eighteen months, we've come a long way working out training pipeline bottlenecks. Additionally, over the next two and a half years of the Cyber Mission Force build, the Services must continue for the Services to incorporate USCYBERCOM training requirements into their training programs, and ensure their workforce meets the CMF standards.

If confirmed, one of my first priorities will be to work closely with NSA and the Services to expand existing training classes, identify training equivalencies, and establish alternate training venues. I think we should also look collectively at increasing the time on station requirements to retain trained and fully qualified personnel until sufficient training programs are in place.

What direction has been given to the services regarding recruiting goals and priorities for individuals with skills and aptitudes relevant to the needs of CYBERCOM?

Senior DoD leadership directed the Services to establish management processes that identify, recruit, retain and provide incentivized career advancement paths for military and civilian personnel. This allows the high-end advanced skills that United States Cyber Command has identified to work in the Cyber Mission Force. Progress is being made by each Service and the issue is monitored closely in monthly reporting by USCYBERCOM to the Joint Staff. DoD is addressing one of the more significant challenges by looking at options pertaining to the civilian workforce that would establish a flexible and responsive workforce that improves the ability to attract, develop, motivate and retain a high quality Cyber workforce.

Has the Department considered delegating personnel authorities to CYBERCOM that are similar to those that are exercised by U.S. Special Operations Command to ensure that the Services manage the careers of their service members with cyber skills appropriately?

USSOCOM's Article 167 Authorities continue to prove essential to their ability to work with the Services to develop truly Joint capabilities that meet Joint Standards. USCYBERCOM continues to do a great job facilitating progress without such authority, but eventually delegating these authorities could greatly enhance their ability to meet the nation's needs.

What would be the pros and cons of providing CYBERCOM such authorities?

While there are no real cons in my opinion, the pro for CYBERCOM is the same as for SOCOM. This authority would allow CYBERCOM to shape the cyber force and ensure cyber training and capabilities are standardized and inherently Joint across the man, train, and equip spectrum. Once trained, these personnel are highly skilled and valuable commodities. They are bona fide high-demand, low-density assets - just as our Special Operations Forces are.
We are growing a highly skilled, highly qualified standardized workforce.

CYBERCOM, empowered with these types of authorities can more effectively advocate and ensure that we do everything in our power to retain these exceptional forces even as our manpower, promotion, and retention systems may be slow to recognize this.

Designing the Internet for Better Security

How could the Internet be redesigned to provide greater inherent security?

Advancements in technology continually change the architecture of the Internet. Cloud computing, for instance, is a significant change in how industry and individuals use Internet services. As evidenced by the growth of security conferences, companies and media attention, security is at the forefront of Internet use as businesses and government strive to protect intellectual property and citizens desire to protect their privacy. To put it simply, the environment is ripe for significant attention to inherent security and government, industry and academia all have an interest in achieving this objective.

I believe there are options for the Internet to provide greater inherent security. Several major providers of Internet services are already implementing increased security in email and purchasing services by using encryption for all transmissions from the client to the server. It is possible that the service providers could be given more responsibility to protect end clients connected directly to their infrastructures. They are in a position to stop attacks targeted at consumers and recognize when consumer devices on their networks have been subverted. The inability of end users to verify the originator of an email and for hackers to forge email addresses have resulted in serious compromises of end user systems. If confirmed, I look forward to working with this Committee, as well as industry, academia and government leaders, on the advancement of security measures for the Internet.

Is it practical to consider adopting those modifications?

I believe modifications to enhance security on the Internet will evolve and strengthen over time. Industry is developing and deploying solutions today to maintain the trust of their clients. Events such as recent payment card breaches are highlighting the concerns and accelerating solution deployment. These advancements in commercial technologies provide a benefit to all who use them, including government. Public-private working groups have and will continue to address hard problems and implementable solutions to strengthen security on the Internet.

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

I believe the government should strive to implement advanced security measures that enhance privacy. Tensions between security and privacy are not new, but I believe we cannot accept one without the other. Increased security should help protect identities, reduce cyber attacks, and assure the transmission and storage of private data; in turn, this enhanced security will ultimately improve individual and corporate privacy in the Internet. If confirmed, I look forward to working with this Committee and industry and government leaders to protect privacy while making the Internet as secure as possible.

The Section 215 Program

In January, 2014, the President ordered a transition to end the Section 215 telephone metadata collection program as it currently exists, to "preserve the capabilities we need" without the government collecting and holding the data on call detail records.

What are your views on what specific capabilities need to be preserved as the program is transitioned?

The program grew out of a desire to address a gap identified after 9/11. One of the 9/11 hijackers -- Khalid al-Mihdhar -- made a phone call from San Diego to a known al Qaeda safe-house in Yemen. NSA saw that call, but it could not see that the call was coming from an individual already in the United States. The telephone metadata program under Section 215 was designed to map the communications of terrorists so we can see who they may be in contact with as quickly as possible. It does not involve the content of phone calls or the names of the people making the calls.

I believe that we need to maintain an ability to make queries of phone records in a way that is agile and provides results in a timely fashion. Being able to quickly review phone connections associated with terrorists to assess whether a network exists is critical.

From your perspective, what are the pros and cons, and problems, involved in the establishment or designation of a private "third party" to hold the data, on the one hand, and the service providers keeping the data, on the other?

Both options are technically feasible and, if implemented in a manner that addresses mission requirements, could be viable alternatives for the current program. I anticipate that either would require significant up-front costs. However, if a private "third party" holds the data, I expect it would be at greater expense and could introduce other complexities. For example, as the President noted in his speech on 17 January 2014, it could require companies to alter their procedures in ways that raise new privacy concerns. If the service providers keep the data, I understand that this may require statutory changes for any data retention requirements which may be levied upon them.

What is your assessment of the impact on the program of the President's order to have the FISA Court make individual RAS determinations prior to non-emergency database queries?

Before the President's speech on January 17, 2014, this approval process was done internally at NSA and both DOJ and ODNI conducted post-approval reviews of RAS determinations on a quarterly basis. Since 17 January, NSA has been working closely with DOJ to establish processes and procedures to obtain RAS approvals from the FISA court.

The Federal Communications Commission requires service providers to keep telephone call detail records for 18 months. The government currently keeps the records collected under section 215 for 5 years. Section 215 expires next year. If Congress does not renew the provision, the executive branch could continue to access call records under other authorities, but only through the service provider's repositories.

Is that a viable alternative?

The other authorities, as currently established, do not fully replicate the current ability under Section 215 to obtain telephony metadata records in a way that is agile and timely. However, I believe it's possible that, if new legal authorities were established or existing authorities were modified to enable more flexible acquisition of such records, these could serve as a viable alternative.

How critical is it in your opinion to have guaranteed access to records more than 18 months old from all service providers?

Currently, NSA retains the metadata for five years, but it is my understanding that NSA has assessed that the five-year retention period could be reduced to a shorter period without significantly decreasing operational utility. In his January speech, the President directed a study of how to restructure the program for the longer term. The work of that study, with participants from multiple agencies, is now ongoing. While specific options are under development, there is further work to be done.

What concerns do you have, if any, about leaving the metadata records with the service providers, and having them produce records responsive to Court-approved queries?

My main concern is whether such an arrangement would produce records in a timely fashion. Being able to quickly review phone connections associated with terrorists to assess whether a network exists is critical. The ongoing interagency review is looking at ways to address this risk.

<u>Section 215 Utility Versus Privacy Concerns</u>

The Privacy and Civil Liberties Oversight Board (PCLOB) and the President's Review Group On Intelligence and Communications Technologies ("Review Group") characterized the Section 215 program as useful but not critical. The PCLOB stated that "We have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation."

What is your understanding of the utility of the program, and how that utility compares to the level of concern among the American people about its perceived impact on privacy and civil liberties?

One of the key vulnerabilities identified after 9/11 was the lack of a sufficient and timely capacity to detect when a known foreign based terrorist threat was in contact with someone

inside the homeland. The Section 215 program was designed to provide that capability by enabling the government to quickly review telephone connections to assess whether a terrorist network exists and the President has stated that it is critical the capability that this program was designed to meet is preserved. The President has also been clear about expectations that such a capability be conducted in a manner that addresses the concerns of the American people about the potential impact on privacy and civil liberties. I support the ongoing interagency effort in response to the President's direction to seek to find an ability for this necessary capability to exist within an acceptable privacy and civil liberties regime.

The Review Group also stated on multiple occasions that the 215 program, contrary to many public reports, actually only collects "a small percentage of the total telephony metadata held by service providers."

How do the costs compare for expanding the government's capacity to ingest all telephony call records, on the one hand, versus the cost of enabling comprehensive access to needed records through the service providers, on the other?

In the summer and fall of 2013, NSA performed some analysis of the relative costs of having the government collect the data in bulk with the costs of searching data retained at the providers. I have not been briefed on the details or the results of that analysis, or how it might apply to specific proposals now under consideration. If I am confirmed for this position, it will be my responsibility to thoroughly and accurately communicate costs and benefits to those who set policy and establish appropriations. Cost will be a factor taken into consideration in the development of options for the President. If confirmed, I will ensure that Congress will be informed of the cost of any successor programs.

Reform of the FISA Court

The President's Signals Intelligence Directive (PPD-28) announced in January called for Congress to authorize a panel of advocates from outside the government to "provide an independent voice in significant cases" before the FISA Court. A similar approach has been recommended by the PCLOB and the President's Review Group.

Do you have any concerns about introducing an adversarial element in the proceedings of the FISA Court as the President and others have urged?

I concur with the President's view that responsible actions which will help increase the transparency of and confidence in the government's conduct of extraordinary authorities--like those performed under statutory authority with the Foreign Intelligence Surveillance Court--are an important element of government's relationship with the American people. If the legislative and judicial branches of government introduce changes to the FISA court or its proceedings, and if I am confirmed, I will be fully prepared to work with them and alongside others in the executive branch. Whatever approach is considered, I believe must also address the necessary timeliness and operational integrity of national security activities.

Standards for Searching NSA Databases Using U.S. Persons' Personally Identifiable Information

NSA collects foreign intelligence information under multiple authorities, including Executive Order 12333, traditional individualized FISA Court orders, and programs such as section 702 of the FISA Amendments Act, and section 215 of the Patriot Act. Unlike EO 12333 collection, traditional FISA wiretaps must meet a probable cause standard and are very specifically targeted. The section 215 program involves bulk collection, but only of non-content metadata, and the bulk data is queried under the Reasonable, Articulable Suspicion (RAS) standard that the target of the query is associated with terrorist groups. Section 702 content collection is based on the "reasonable belief" standard that the specific target of the collection is a non-U.S. Person located outside the United States. The President's Review Group On Intelligence and Communications Technologies ("Review Group") and the PCLOB have raised issues about the standards under which the government can search through data holdings acquired under these authorities using U.S. Persons identifiers.

Is NSA permitted to search data acquired under EO 12333 authorities using U.S. Persons identifiers without probable cause?

Signals intelligence information acquired by NSA under EO 12333 must be handled in accordance with the Attorney General-approved minimization procedures that are reasonably designed to protect the privacy interests of United States persons. The full procedures are classified, but generally prohibit selection of the content of communications of or concerning a U.S. person absent probable cause. However, there are exceptions, such as when there is a threat to life or when the search is limited to querying information under which there is no reasonable expectation of privacy (e.g. metadata).

If so, what is your understanding of the legal justification? Does the Review Group's recommendation, relate to or cover queries of data acquired under EO 12333?

I defer to the Department of Justice for any legal interpretation of the procedures approved by the Attorney General.

Is NSA allowed to search data acquired under traditional FISA individual wiretap orders using U.S. Persons identifiers without probable cause?

Information acquired by NSA under traditional FISA orders must be handled in accordance with the Court-approved minimization procedures, as defined by FISA, that are reasonably designed to protect the privacy interests of United States persons. NSA's Court-approved minimization procedures for traditional FISA orders do not permit data searches using U.S. person names or identifiers. Any exceptions to these procedures would require approval by the Federal Intelligence Surveillance Court (FISC).

If so, what is your understanding of the legal rationale?

I defer to the Department of Justice for any legal interpretation of the procedures approved by the FISC for individual FISA wiretap orders.

What is your understanding of the legal rationale for NSA to search through data acquired under section 702 using U.S. Persons identifiers without probable cause?

Information acquired by NSA under Section 702 of FISA must be handled in strict accordance with minimization procedures adopted by the Attorney General and approved by the Foreign Intelligence Surveillance Court. As required by the statute and certifications approving Section 702 acquisitions, such activities must be limited to targeting non-U.S. persons reasonably believed to be located outside the United States. NSA's Court-approved procedures only permit searches of this lawfully acquired data using U.S. person identifiers for valid foreign intelligence purposes and under the oversight of the Department of Justice and Office of Director of National Intelligence.

What is your understanding of the legal rationale for searching through the "Corporate Store" of metadata acquired under section 215 using U.S. Persons identifiers for foreign intelligence purposes?

The section 215 program is specifically authorized by orders issued by the Foreign Intelligence Surveillance Court pursuant to relevant statutory requirements. (Note: the legality of the program has been reviewed and approved by more than a dozen FISC judges on over 35 occasions since 2006.) As further required by statute, the program is also governed by minimization procedures adopted by the Attorney General and approved by the FISC. Those orders, and the accompanying minimization procedures, require that searches of data under the program may only be performed when there is a Reasonable Articulable Suspicion that the identifier to be queried is associated with a terrorist organization specified in the Court's order.

<u>Information Sharing Legislation for Cybersecurity</u>

Several proposed cybersecurity bills have been introduced to authorize the collection and sharing of information on cybersecurity threats -- including malware, command and control, exfiltration of data, and other evidence of compromise – between the public and private sectors for the purpose of enabling the private sector and government defend themselves, enabling law enforcement agencies to detect criminal activities and identify and prosecute perpetrators, and, in the case of nation-states, enabling the government to attribute attacks and hold aggressors accountable. To date, none of these proposals have been enacted.

116. In your view, would it be helpful for Congress to enact more limited legislation to enable the private sector to collect and share cyber threat information within the private sector, leaving the issue of sharing with the government for the future?

The nature of malicious cyber activity against our nation's networks has become a matter of such concern that legislation to enable real-time cyber threat information sharing is vital to protecting our national and economic security. Incremental steps such as legislation that addresses only private sector sharing would have limited effectiveness, because no single public or private entity has all the necessary authorities, resources, or capabilities to respond to or prevent a serious cyber attack. Therefore, we must find a way to share the unique insights held by both government and the private sector. At the same time, legislation must help construct a trust-based community where two-way, real-time sharing of cyber threat information is done consistent with protections of U.S. person privacy and civil liberties.

What restrictions would you recommend be imposed on what information could be shared with the government regarding cyber threats, and the uses to which the government could apply that information?

Protecting the security and the privacy of Americans is not a mutually exclusive proposition. The information provided to the government should be limited to that which is necessary for the government to understand or take action to counter a cyber threat and to which all appropriate mechanisms have been applied to protect the privacy and civil liberties of US persons. If confirmed, I would expect to engage fully in discussions on how to accomplish these objectives.

What transparency measures and institutional checks would you recommend to increase confidence that allowing the sharing of cyber threat information would not lead to abuses of privacy and civil liberties?

Transparency can be ensured by establishing procedures for receiving, retaining, using, and disclosing cyber threat information. In turn, compliance with these procedures should be subject to independent review and oversight by cleared trusted U.S. Government and private sector third parties. Due to the criticality of real-time sharing of cyber threat information, we must also leverage technology that enables a transparent, policy-based, machine-speed infrastructure that automatically enforces the rules for use and any lawful restrictions on sharing.

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.

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

Yes

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

Yes

Do you agree, if confirmed, to appear before this Committee, or designated members of this Committee, and provide information, subject to appropriate and necessary security protection, with respect to your responsibilities as Commander, U. S. Cyber Command?

Yes

Do you agree to ensure that testimony, briefings and other communications of information are provided to this Committee and its staff and other appropriate Committees?

Yes

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

Yes