Advance Questions for Eric Rosenbach
Nominee for the Position of Assistant Secretary of Defense for Homeland Defense

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?

I do not see a need to amend any provisions of the Goldwater-Nichols Act. Since its adoption in 1986, Goldwater-Nichols has met its intended goals of improving civilian oversight of the Department of Defense (DoD) and creating a joint environment among the Services.

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

Currently, I do not believe that modification to the Goldwater-Nichols Act is required.

Duties and Qualifications

DOD Directive 5111.13 of January 16, 2009 states that the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA)), "under the authority, direction, and control of the Under Secretary of Defense for Policy (USD(P)), serves as the principal civilian advisor to the Secretary of Defense and the USD(P) on homeland defense activities, Defense Support of Civil Authorities (DSCA), and Western Hemisphere security matters." It further elaborates that the ASD(HD&ASA) shall provide overall supervision of homeland defense activities of the Department of Defense (DOD) which include "Defense Critical Infrastructure Program (DCIP); domestic antiterrorism; the Defense Continuity Program; other homeland defense-related activities; and alignment of homeland defense policies and programs with DOD policies for counterterrorism and counternarcotics."

The Secretary of Defense has announced a plan to reorganize the Office of the Under Secretary of Defense for Policy, under which the ASD for Homeland Defense is located. What is your understanding of the duties and functions of the Assistant Secretary of Defense (ASD) for Homeland Defense position to which you have been nominated,

and do they differ from those described in DOD Directive 5111.13?

My understanding of the duties and functions of the Assistant Secretary of Defense for Homeland Defense is consistent with those described in DoD Directive 5111.13, as well as other applicable DoD directives, with the exception of the duties and functions for Western Hemisphere security policy, which has been transferred within the Office of the Under Secretary of Defense for Policy to the Assistant Secretary of Defense for International Security Affairs (ASD(ISA)). In the future, the Assistant Secretary of Defense for Homeland Defense will assume some of the duties and functions currently assigned to the Assistant Secretary of Defense for Global Strategic Affairs (ASD(GSA)), including the duties and functions for cyberspace, space, and countering weapons of mass destruction policies.

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

My professional background includes nearly twenty years of experience working on national security issues in the military, private sector, academia, and Federal Government. I believe that both my substantive expertise and leadership experience provide me with the background necessary to serve successfully, if confirmed, as Assistant Secretary of Defense for Homeland Defense.

My substantive background includes extensive practical and academic work in intelligence, counterterrorism, homeland security, and cyber policy. As the commander of an Army intelligence unit, I gained invaluable experience about military and intelligence operations. I gained a deep understanding of U.S. counterterrorism and homeland security efforts as a professional staff member on the Senate Intelligence Committee. At the Harvard Kennedy School, I taught classes on national security policy and authored a book focusing on counterterrorism. Over the last two and one-half years at the Pentagon, I gained a deep understanding of the cybersecurity challenges facing the nation.

I believe that I also have the strong leadership and management skills necessary to serve effectively as Assistant Secretary. As a senior executive at a large international telecommunications firm, for example, I managed complex projects across fifteen nations. Later, I served as the Executive Director of a large center at the Kennedy School, where I was responsible for managing all aspects of the center's operations. Prior to my work in the Pentagon, I was a senior executive at an international consulting firm working with Fortune 500 executives.

What additional actions do you believe you need to take, if any, to prepare yourself to fulfill these duties?

If confirmed, I am prepared to undertake fully the duties and functional areas within the Office of the Assistant Secretary of Defense for Homeland Defense and anticipate working with the congressional defense committees to fulfill my responsibilities under Title 10.

Relationships

What do you see as the relationship between the Assistant Secretary of Defense for Homeland Defense and each of the following:

The Secretary of Defense

Under the authority, direction, and control of the Under Secretary of Defense for Policy (USD(P)), the Assistant Secretary of Defense for Homeland Defense serves as the principal civilian advisor to the Secretary of Defense on homeland defense activities and Defense Support of Civil Authorities. In the future, I understand that this responsibility will expand to serving as the principal civilian advisor on DoD cyber, space, and countering weapons of mass destruction policy.

The Deputy Secretary of Defense

The Assistant Secretary of Defense for Homeland Defense provides support to the Deputy Secretary similar to that provided to the Secretary, as described above.

The Under Secretary of Defense for Policy

The Assistant Secretary of Defense for Homeland Defense functions under the authority, direction, and control of the USD(P) and provides the USD(P) with advice and support on homeland defense policy formulation, interagency deliberations, engagement with interagency interlocutors, and the Planning, Programming, Budgeting, and Execution (PPBE) processes and strategic reviews within the Department. In the future, the ASD's role will be expanded to include DoD cyber, space, and countering weapons of mass destruction policy matters.

The Under Secretary of Defense for Intelligence

Under the authority, direction, and control of the USD(P), the Assistant Secretary of Defense for Homeland Defense works closely with the Under Secretary of Defense for Intelligence (USD(I)) to achieve the Secretary of Defense's objectives, particularly the defense of the United States from attack upon its homeland.

The Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict

The Assistant Secretary of Defense for Homeland Defense works closely with the Assistant Secretary of Defense for Special Operations & Low-Intensity Conflict to provide the USD(P) and the Secretary of Defense with advice and recommendations on policy issues regarding combating terrorism within the United States and homeland defense policy oversight to ensure that the Secretary's guidance and decisions are implemented.

The Assistant Secretary of Defense for International Security Affairs

The Assistant Secretary of Defense for Homeland Defense works closely with the ASD (ISA) to provide the USD(P) and the Secretary of Defense with advice and recommendations on issues regarding emerging threats to the United States and homeland defense policy oversight to ensure that the Secretary's guidance and decisions are implemented.

The Assistant Secretary of Defense for Reserve Affairs and the civilian officials of the military departments in charge of Reserve affairs

The Assistant Secretary of Defense for Homeland Defense works closely with the Assistant Secretary of Defense for Reserve Affairs and civilian officials of the Military Departments in charge of reserve affairs in the areas of DoD policy regarding the development, readiness, and employment of National Guard and other Reserve Component forces within the United States, as well as homeland defense policy oversight to ensure that the Secretary of Defense's guidance and decisions are implemented properly.

The Chief of the National Guard Bureau, and the Directors of the Army and Air National Guard

The Assistant Secretary of Defense for Homeland Defense works closely with the Chief of the National Guard Bureau, and the Directors of the Army and Air National Guard, on the roles, capabilities, and readiness of the National Guard to support the homeland defense and civil support priorities and objectives of the Secretary of Defense.

The Director of the Defense Intelligence Agency

Under the authority, direction, and control of the USD(P), the Assistant Secretary of Defense for Homeland Defense works closely with -- and provides advice on homeland defense, Defense Support of Civil Authorities, DoD cyber, space, and countering weapons of mass destruction policy to -- the Director of the Defense Intelligence Agency to achieve the Secretary of Defense's objectives in defense of the United States.

The Chairman and Vice Chairman of the Joint Chiefs of Staff and the Joint Staff

As the principal military advisor to the Secretary of Defense, the President, the National Security Council, and the Homeland Security Council, the Chairman of the Joint Staff (CJCS) has a unique and critical military role. If confirmed as the Assistant Secretary of Defense for Homeland Defense, I would work closely with the Chairman and Vice Chairman to support the efforts of the Secretary and Deputy Secretary, and to ensure that their military advice is taken into account in an appropriate manner.

The Commander of United States Northern Command and the North American Aerospace Defense Command

The Assistant Secretary of Defense for Homeland Defense works closely with the Commander of the North American Aerospace Defense Command and U.S. Northern Command (USNORTHCOM) to support the efforts of the Secretary, Deputy Secretary, and USD(P), particularly in the areas of homeland defense, Defense Support of Civil Authorities strategy and policy, contingency planning, and policy oversight of operations.

The Commander of United States Pacific Command

The Assistant Secretary of Defense for Homeland Defense works closely with the Commander of the U.S. Pacific Command (USPACOM) to support the efforts of the Secretary, Deputy Secretary, and USD(P), particularly in the areas of homeland defense and Defense Support of Civil Authorities strategy and policy, contingency planning, and policy oversight of operations.

At the direction of the USD(P) and in coordination with the CJCS, the Assistant Secretary of Defense for Homeland Defense works with the Commander of USPACOM on a broad range of issues that affect strategy and policy for countering the proliferation of weapons of mass destruction, as well as for the space and cyberspace domains.

The Commander of United States Strategic Command

At the direction of the USD(P) and in coordination with the CJCS, the Assistant Secretary of Defense for Homeland Defense works with the Commander of U.S. Strategic Command (USSTRATCOM) on a broad range of issues that affect strategy and policy for countering the proliferation of weapons of mass destruction, as well as for the space and cyberspace domains.

The Commander of United States Cyber Command

At the direction of the USD(P) and in coordination with the CJCS, the Assistant Secretary of Defense for Homeland Defense works with the Commander of U.S. Cyber Command (USCYBERCOM) on a broad range of issues that affect the Department’s

activities in cyberspace. As I understand it, once duties that are currently performed by the Assistant Secretary of Defense for Global Security Affairs (OASD(GSA)) become part of the responsibilities of the Assistant Secretary of Defense for Homeland Defense, the Assistant Secretary of Defense for Homeland Defense would provide senior-level civilian oversight of U.S. Cyber Command. If confirmed, I look forward to continuing to ensure that the relationship with USCYBERCOM remains close and would facilitate coordination as the Department's role in the cyber domain evolves.

The Director of the Defense Threat Reduction Agency

The Assistant Secretary of Defense for Homeland Defense, in coordination with the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, works closely with the Director of the Defense Threat Reduction Agency (DTRA), particularly regarding efforts in chemical, biological, radiological, and nuclear threat reduction and defense, counter-proliferation, and emergency response support and training. This close coordination is necessary to ensure that the Assistant Secretary of Defense for Homeland Defense is able to provide policy oversight and guidance to the Department of Defense's Cooperative Threat Reduction Program, which is implemented by DTRA.

The Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs

The Assistant Secretary of Defense for Homeland Defense works closely with the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (ASD(NCB)) on DoD's chemical, biological, and nuclear defense programs as they relate to homeland defense, antiterrorism/force protection, and Defense Support of Civil Authorities.

The Department of Homeland Security

The Assistant Secretary of Defense for Homeland Defense (and my current office) has a close working relationship with the Department of Homeland Security due to the complementary responsibilities of homeland defense and homeland security missions and the need for a close, habituated, and well-exercised relationship for the rapid execution of Secretary of Defense-approved defense support of civil authorities missions as requested by the Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA).

The State Governors

The Assistant Secretary of Defense for Homeland Defense serves as the principal DoD representative to State Governors on policy matters pertaining to homeland defense activities, Defense Support of Civil Authorities, and DoD security matters, including but not limited to: defense domestic consequence management; activities commonly referred to as mission assurance (Defense Critical Infrastructure Program, Defense Continuity

Program, Defense Crisis Management); the alignment of homeland defense activities with counterterrorism and counternarcotics policy and programs; and DoD cyberspace activities, space policy, and WMD counter-proliferation.

In 2010, the Secretary of Defense designated the Assistant Secretary of Defense for Homeland Defense as the Executive Director of the Council of Governors. If confirmed, I would, as Executive Director, be responsible for coordinating the activities of the Council.

Major Challenges and Problems

In your view, what are the major challenges that will confront the ASD for Homeland Defense?

If confirmed, my primary challenge and top priority would be to continue and improve the outstanding efforts the Department of Defense has devoted to protecting the homeland from a major terrorist attack. I would be particularly focused on preventing an attack using a weapon of mass destruction and on planning and preparing for the response to catastrophic incidents in the United States, including weapons of mass destruction (WMD).

One of the most pressing challenges that I would immediately face, if confirmed, once duties of OASD (GSA) are transferred to the Office of the Assistant Secretary of Defense for Homeland Defense, would be managing the Department's efforts to help eliminate Syria's chemical weapons.

I believe that DoD has a crucial role in planning for complex catastrophic incidents; thus, I would devote extensive attention to the Department's preparations for catastrophes like Super Storm Sandy.

If confirmed, I would also devote special attention to the challenge of building the cyberspace workforce, growing DoD's operational capabilities, and continuing to rationalize the complex funding streams that support cyberspace initiatives.

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

If confirmed, I would maintain support for the key issues I outlined above by actively addressing them in key Department of Defense and interagency processes, including the PPBE processes, strategic reviews inside the Department, and the Interagency Policy Committee (IPC) process.

Once duties that currently reside in OASD(GSA) become part of the responsibilities of the Assistant Secretary of Defense for Homeland Defense, I would address challenges in cyberspace initially by streamlining senior-level oversight of workforce, capabilities, and funding issues to improve efficiency throughout the Department for how the cyber force is organized, trained, and resourced.

I am committed to continuing my close working relationships with partners across DoD, with other departments and agencies throughout the executive branch, and with the Congress, to address whatever issues and concerns arise to implement the new policies and strategies.

What do you anticipate will be the most serious problems in the performance of the responsibilities of the ASD for Homeland Defense?

If confirmed, I would initially focus my efforts on the changes that will be made to the Office of the Assistant Secretary of Defense for Homeland Defense as a result of the reorganization of the Office of the Under Secretary of Defense for Policy that Secretary Hagel announced last December. There are many synergies that will occur as a result of this reorganization and, if confirmed, I would ensure that we maximize the collective talents of the staff in the new Homeland Defense organization.

If confirmed, what management actions and timelines would you establish to address these problems?

If confirmed, and upon implementation of the reorganization of the Office of the Under Secretary of Defense for Policy, I would work with each Deputy Assistant Secretary of Defense under the Assistant Secretary of Defense for Homeland Defense to identify the synergies between the homeland defense issues and cyberspace, space, and WMD policy issues and establish a unified vision for the organization.

Combating Terrorism Roles and Responsibilities

Section 902 of the National Defense Authorization Act for Fiscal Year 2003, which established the position of Assistant Secretary of Defense for Homeland Defense, also transferred the responsibility for the "overall direction and supervision for policy, program planning and execution, and allocation and use of resources for the activities of the Department of Defense for combating terrorism" to the Under Secretary of Defense for Policy.

Please specify what combating terrorism activities will be under the jurisdiction of the Assistant Secretary of Defense for Homeland Defense, particularly domestic antiterrorism activities.

It is my understanding that the specific counterterrorism activities that reside under the

Assistant Secretary of Defense for Homeland Defense include providing critical staff support to the Secretary of Defense regarding support requested by the Attorney General, or as directed by the President of the United States to combat domestic terrorism. Also, as I understand it, the Assistant Secretary of Defense for Homeland Defense advises the Secretary of Defense on all domestic consequence management matters.

What DOD official or officials will be responsible for DOD combating terrorism activities not under the jurisdiction of the ASD for Homeland Defense?

The Under Secretary of Defense for Policy has the overall lead for DoD combating terrorism policy oversight. If confirmed, I would work closely with the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD(SO/LIC)) and the Under Secretary of Defense for Intelligence (USD(I)) to achieve the Secretary of Defense's objectives and proper alignment of DoD combating terrorism activities.

The Geographic Combatant Commanders have tactical control (TACON) for Force Protection of all DoD personnel within their areas of responsibility, with the exception of DoD personnel for whom the chiefs of U.S. diplomatic missions have security responsibility. If confirmed, I would work closely with both the Combatant Commanders and the Department of State to ensure that all DoD personnel serving overseas, including those at U.S. missions and embassies, have appropriate anti-terrorism protection.

What steps will you take to ensure that the Department's efforts are focused and well-coordinated in this critical area of homeland defense?

If confirmed, I would work closely with the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and the Under Secretary of Defense for Intelligence to achieve the Secretary of Defense's objectives in this critical area of homeland defense.

I would also use DoD's Mission Assurance Coordination Board, which the ASD for Homeland Defense leads, to ensure that the Department's efforts are focused and coordinated on antiterrorism and force protection issues. DoD's Mission Assurance Senior Steering Group integrates mission-related security issues of mutual interest with other executive committees and efforts within the Department.

Difference Between Homeland Defense and Homeland Security

The Department of Defense is responsible for Homeland defense, and the Department of Homeland Security is responsible for Homeland security.

Please describe your understanding of the differences between the two different missions.

The Department of Defense is responsible for the protection of U.S. sovereignty, territory, population, and critical infrastructure against external threats and aggression, or other threats as directed by the President. The Department's missions are executed to deter, defend against, and defeat those who threaten the United States.

The Department of Homeland Security (DHS) leads the Nation's efforts to prepare for, protect against, respond to, recover from, and mitigate against the risk of terrorist acts, natural disasters, and other natural and manmade disasters. DHS also secures the Nation's borders, ports, and airports; and ensures that the Federal Government works with States, localities, and the private sector as a partner in prevention, mitigation, and response.

As necessary, and consistent with the law, DoD provides support to DHS in the execution of its missions.

Do you agree that the Department of Defense should not be responsible for Homeland security, but may serve in a supporting role to assist civilian federal agencies, as directed by the President or Secretary of Defense?

Yes. In enacting the Homeland Security Act of 2002, Congress assigned responsibility to DHS for preventing terrorist attacks within the United States; reducing the vulnerability of the United States to terrorism; and minimizing the damage and assisting in the recovery from, terrorist attacks within the United States. As necessary, and consistent with the law, DoD provides support to DHS in the execution of its missions.

Relationship with the Department of Homeland Security

The establishment of the Department of Homeland Security was one of the U. S. Government's largest cabinet-level reorganizations in the last 50 years. Despite this reorganization, the Department of Defense will continue to play an important role in providing Defense Support of Civil Authorities for federal response to certain domestic incidents, as directed by the President or the Secretary of Defense.

Please describe your understanding of the relationship between the Department of Defense and the Department of Homeland Security, particularly with respect to Defense Support of Civil Authorities and cyber security.

DoD has a strong, mutually supporting relationship with DHS that dates back to its inception. As I understand it, the preponderance of requests for assistance that the Department receives comes from one of DHS's operational components. Since the Office of the Assistant Secretary of Defense for Homeland Defense was created in 2003, the Federal Emergency Management Agency (FEMA) has submitted to DoD more requests for assistance than all

other sources combined. The Secret Service, Customs and Border Protection, and the Coast Guard have also made multiple requests each year.

In the area of cyber security, the Department of Defense provides personnel, equipment, and facilities in order to increase interdepartmental collaboration in strategic planning for the nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities. The formal Memorandum of Agreement between the Departments focuses national cybersecurity efforts to increase the overall capacity and capability of both DHS's homeland security and DoD's national defense missions, while providing integral protection for privacy, civil rights, and civil liberties.

If confirmed, what role do you expect to play in the direction and coordination of DOD activities with the Department of Homeland Security and its component elements?

If confirmed, I would build on the strong professional relationships that have been developed between the Departments. I would represent DoD in senior-level discussions with colleagues from DHS and its operational components. I understand that key areas of collaboration and coordination include working with the U.S. Coast Guard on maritime domain awareness, Customs and Border Protection on support to border security, the Secret Service on Presidential and dignitary protection, and DHS's Office of Cyber Security and Communications on national cyber policy.

Defense Support of Civil Authorities

The ASD for Homeland Defense has primary responsibility for Defense Support of Civil Authorities (DSCA), particularly support to the Department of Homeland Security and its components, for response to natural and man-made disasters in the United States.

Please describe your general understanding of the roles and responsibilities of the Department of Defense in providing DSCA, and the roles and responsibilities of other federal agencies in responding to domestic disasters.

Defense Support of Civil Authorities is one of the primary missions of the Department as articulated in the latest National Defense Strategy, "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense," dated January 2012. When directed by the President or approved by the Secretary of Defense, the Department has robust capabilities and capacity that can be used to support civilian authorities at the Federal, State, and local levels.

For domestic emergencies and disasters, FEMA has statutory responsibility to coordinate the Federal support to State, tribal, and local authorities. When requested by FEMA, or when directed by the President or Secretary of Defense, the vast capabilities of the Department can be used to supplement FEMA support to local, tribal, State, and other Federal departments and

agencies.

Under current law, when the Department of Defense provides Defense Support to Civil Authorities, what are the responsibilities of other federal agencies for paying for or reimbursing the Department for such support?

During an emergency or disaster, when the Department is asked to support FEMA under the terms of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, the Department is reimbursed by FEMA for civilian overtime, temporary duty expenses, and the operational and maintenance costs of providing the support. DoD is not reimbursed for the pay and allowances of personnel providing the support.

Under the Presidential Protection Assistance Act of 1976, when the Department provides temporary support to the Secret Service that is directly related to the protection of the President or Vice President, the support is provided on a non-reimbursable basis. When support is provided to the Secret Service for other protected persons, DoD is reimbursed for its expenses.

When we support other Federal departments and agencies under the Economy Act (Title 31, U.S. Code, Section 1535), DoD is reimbursed for all of our support costs, including the pay and allowances of the personnel providing the support.

Defense Critical Infrastructure Program

The ASD for Homeland Defense is responsible for overseeing DOD efforts and programs to protect defense critical infrastructure in the United States.

If confirmed, what plans, approaches, and priorities would you have for ensuring that the Defense Critical Infrastructure Program is functioning properly?

I am familiar with the importance of the Defense Critical Infrastructure Program (DCIP) and worked closely with this program while leading the Cyber Policy office. If confirmed, one of my priorities would be to integrate this program further with other risk management programs across the Department to ensure DoD's ability to execute missions. I would review such plans, approaches, and priorities, and make recommendations to the USD(P) to ensure that adequate measures are taken for the protection of defense critical infrastructure in an all-hazards environment to ensure mission execution.

Installation Security

The security of U.S. military installations - both at home and abroad - has been a longstanding priority for the Senate Armed Services Committee.

If confirmed, what would be your priorities for ensuring an adequate level of security for military installations in the United States?

If confirmed, I would work to ensure the effectiveness of Department of Defense antiterrorism and protection policies in detecting, deterring, and responding to threats directed at DoD installations, facilities, and personnel, including their families. I would also work to ensure that adequate resources are provided to execute these policies and that the Department of Defense is working closely with its Federal, State, local, and tribal partners in establishing a mutually supportive protective posture inside and outside DoD installations and facilities.

Although the Under Secretary of Defense for Intelligence is the principal staff assistant for physical security, if confirmed, I would support an antiterrorism approach to physical security, focused on risk mitigation, which defends in-depth using technology and manpower to reduce risk and mitigate potential threats. In addition, I would encourage DoD Components to share access control information and continuously vet individuals against U.S. criminal and terrorist databases. Moreover, I would help to ensure that antiterrorism policy is consistent with DoD physical security and installation emergency management policy, as part of the overall DoD Mission Assurance effort.

Defense Continuity and Mission Assurance

The ASD for Homeland Defense has primary responsibility for the Defense Continuity Program and for DOD Mission Assurance in the United States.

What is your understanding of the roles and responsibilities of the ASD for Homeland Defense with respect to the Defense Continuity Program and Mission Assurance?

It is imperative that the Department has the ability to provide senior leaders a clear understanding of risks to mission accomplishment and that we possess the tools and processes needed to develop effective options to reduce associated risks. Defense Continuity and Mission Assurance provide this important capability to ensure resiliency and readiness.

Under the authority, direction, and control of the USD(P), the Assistant Secretary of Defense for Homeland Defense has two major responsibilities for the Defense Continuity Program. The first is to develop, coordinate, and oversee implementation of Defense continuity policy (which includes activities supporting continuity of operations, continuity of government, and enduring constitutional government). The second is to develop and oversee a comprehensive continuity program, including continuity plans to support the Secretary, the Deputy Secretary, and their senior and supporting staffs, and

the DoD Components in coordination with the Chairman of the Joint Chiefs of Staff.

If confirmed, what would be your priorities for accomplishing these important missions?

If confirmed, one of my mission assurance priorities would be to review how DoD prioritizes risk mitigation efforts to eliminate unnecessary redundancies, achieve closer integration of key activities, and more effectively inform the resourcing of existing programs and future investments related to mission assurance.

If confirmed, one of my Defense Continuity Program priorities would be to continue modernization of selected DoD continuity capabilities to improve readiness and resilience while incorporating operational efficiencies.

CBRN Consequence Management Enterprise

Among the specialized capabilities that the Defense Department can provide to civil authorities are the Chemical, Biological, Radiological, and Nuclear (CBRN) consequence management response forces. These comprise a mix of National Guard and Active Component forces and units, both large and small.

Please describe your understanding of the composition and role of the DOD CBRN consequence management enterprise, the circumstances under which they could be used, and the role of National Guard capabilities in responding to both state and federal CBRN incidents.

The consequence management enterprise is composed of approximately 18,500 Active and Reserve Component forces on alert to support civilian authorities in rapidly responding to mitigate the consequences of a domestic CBRN incident (e.g., nuclear plant, chemical facility, or biological attack).

Consequence management enterprise capabilities reside in the Active Components and Reserve Components, including National Guard forces under State command and control (some of which are DoD-funded). Maintaining capabilities in the National Guard better enables a rapid response in support of local and State responders.

Each State and territory hosts at least one National Guard Weapons of Mass Destruction-Civil Support Team, and there are larger, regionally positioned National Guard forces, including CBRN Enhanced Force Packages and Homeland Response Forces, all prepared to provide immediate response capabilities, including casualty search and extraction, medical triage, and decontamination.

If confirmed, what would be your role with regard to the oversight, training, certification,

coordination, and employment of the Defense Department's CBRN consequence management response forces?

As I understand it, elements of the CBRN force participate in ambitious training, standardization, and evaluation programs. If confirmed, I would work closely with USNORTHCOM and the National Guard Bureau to ensure that DoD's consequence management forces maintain their full operational capability.

Cyber Security

You are currently the DASD for Cyber Policy, and have experience working with the Department of Homeland Security and other federal agencies that have domestic cyber security responsibilities. The planned reorganization of the Office of the Under Secretary of Defense for Policy envisions the ASD for Homeland Defense having primary responsibility for Department of Defense cyber security policy.

What is your understanding of the roles and responsibilities of the Department of Defense for cyber security, and how do they compare to the roles and responsibilities of the Department of Homeland Security?

Ensuring the nation's cybersecurity is a shared responsibility across the U.S. Government. DHS is the lead Federal department responsible for national protection against, mitigation of, and recovery from domestic cybersecurity incidents, for which both DOJ and DoD provide support. DHS is further responsible for the security of unclassified Federal civilian systems. DOJ is responsible for the investigation, attribution, disruption, and prosecution of cyber crimes outside of military jurisdiction. All three Departments share cybersecurity information with each other, and each coordinates with public, private, and international partners.

DoD is responsible for defending the nation from attack in all domains, including cyberspace. As such, DoD plans, coordinates, and conducts cyberspace operations to operate and defend DoD critical infrastructure and military systems. When directed, DoD can conduct cyberspace operations to defend the nation and defend and enable military actions in all domains. Upon request, DoD may also assist in providing Federal support to the private sector and State and local governments.

Given that cyber threats can be inherently global in nature, and that cyber security is not a mission limited to the Homeland, how do view the relationship of cyber security to homeland defense?

Homeland defense includes the protection of U.S. sovereignty, territory, domestic population, and defense critical infrastructure against external threats and aggression, or against other threats as directed by the President. The Department of Defense is responsible for homeland defense. As with threats to the United States, our allies and

partners, and our interests in other domains, DoD has the mission to defend the nation in cyberspace. Because many cybersecurity threats allow would-be adversaries to attack the nation from overseas, I believe cybersecurity is a key part of homeland defense. Of course, the Department must continue to work with other federal departments and agencies, the private sector, and international partners to ensure the Department can carry out its assigned missions in cyberspace as well as in other domains.

Supervision and Management of the Cyber Mission

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. This official must be responsible for overall supervision of cyber activities, including policy and operational considerations, resources, personnel, and acquisition and technology. This official also must assemble a small cross-functional team to integrate cyber expertise across the Department to enable sound decisions while leaving execution of decisions to existing organizations and officials.

The description of the duties of the office to which you have been nominated provided to the Committee does not mention these responsibilities and authorities.

Has the position to which you have been nominated been designated as the principal cyber advisor to the Secretary? If not, which position has been so designated?

At this time, the Secretary has not formally designated his principal cyber advisor. However, along with many colleagues throughout the Department, I am involved in deliberations that have studied how best to implement this legislation. Once the reorganization of the Office of the USD(P) is complete, the Assistant Secretary of Defense for Homeland Defense will be responsible for cyber policy matters.

How does DOD intend to implement the NDAA legislation? As the incumbent Deputy Assistant Secretary for Cyber in USD(P), have you taken any actions to begin implementation?

Yes, as Deputy Assistant Secretary, I have initiated a Department-wide process to develop options for implementation of the legislation, but the Secretary has not yet made any formal decisions. The opportunity provided by this legislation to streamline oversight of cyber policy within DoD is crucial, so we want to ensure implementation reflects long-term goals for the Department in cyberspace, as well as short-term needs for effective organization and management. We remain mindful of the guidance from the committee contained in the Joint Explanatory Statement that accompanied the legislation.

Infrastructure for U.S. Cyber Command

The National Defense Authorization Act (NDAA) for Fiscal Year 2014 requires the Secretary of Defense to provide U.S. Cyber Command (CYBERCOM) with infrastructure to enable CYBERCOM to independently access global networks to conduct military operations. Congress intends for CYBERCOM to have infrastructure for conducting operations that has attributes that are different from those of the intelligence community, including the ability to scale rapidly, to be disposable, and to cause minimal impacts on our capabilities if discovered by adversaries.

What are your views on this requirement?

I believe that it is essential for USCYBERCOM to have infrastructure that allows it to accomplish military operations that are unique and distinguishable from the intelligence community. Over the past several months, the Department made significant strides in developing plans for diverse, highly-scalable, easily deployable, and disposable platforms, available on demand for the Cyber Mission Force to carry out its missions.

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

DoD has already made significant progress toward achieving this 2014 NDAA requirement. In October 2013, the Deputy Secretary of Defense tasked USCYBERCOM to create a strategy for determining the right mix and number of diverse platforms specifically for use by the Cyber Mission Force. These platforms will provide diversity from the intelligence platform, are able to scale quickly to address specific requirements, and, because they do not need to be overly sophisticated, can be inexpensive to build and deploy.

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

Yes. DoD has already taken large strides toward achieving this 2014 NDAA requirement.

Do you believe this can be implemented in a way that is not redundant or duplicative of existing infrastructure?

It is fiscally prudent for the DoD to leverage all existing capabilities, which is why USCYBERCOM is working with the NSA to ensure there are not duplicative efforts. To ensure the intelligence community can execute its missions free of fear from being exposed by military actions, a USCYBERCOM-dedicated infrastructure on demand is not only reasonable, it is mission critical.

USCYBERCOM is creating a unified architecture plan to ensure there are not redundant

efforts, find ways to leverage previous investments, and ensure the Cyber Mission Force has the infrastructure it needs to carry out its missions. In my current position, I would be happy to provide additional detail about anything related to the "diverse platform" plan in a classified setting at a later time.

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?

I believe, just like in other areas of combat arms, DoD needs to develop its enlisted, officer, and civilian force from a wide variety of career fields, including but not limited to the intelligence and communications communities.

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

Yes. I believe cyber officers, as well as our enlisted forces and civilians should have well-defined career paths focused on operations. Over the past 18 months, the Services have invested extensive attention toward growing our force, and developed plans to recruit and retain our most highly-skilled enlisted and officer forces in the cyberspace operations workforce. Just as we do for other unique military career fields including pilots, cyberspace operators should receive certain incentives to remain in the field. If confirmed, I will continue to work with the Services for cyberspace operations military and civilian forces to be competitive, in both rank and position, with those whose operational focuses have been the other domains.

Alignment of Military Cyber Operations with Cyber Intelligence Collection

For the most part, the military service cyber organizations have been formed from the service cryptologic elements, and in general cyber warfare operations have been regarded as an extension of signal intelligence operations. More recently, however, there is a growing perception that military cyber operations, and the tools and techniques employed in them, should be different from those employed in intelligence operations in cyberspace.

Do you think that, as CYBERCOM matures and as cyber military art develops, military cyber operations and cyber intelligence operations will diverge?

Because the type of targets for military operations may be different than those targets for intelligence operations, I am inclined to think that these operations are likely to diverge in the future. However, a small subset of targets may remain common, such as foreign cyber adversaries.

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

Both communities play vital roles within the services. An important benefit of the distinction is that cyber organizations will tend to have a more explicit focus on warfighting, while cryptologic elements are likely to focus more on their core intelligence-related competencies. However, one drawback of over-emphasizing this distinction would be to neglect the important nexus between warfighting and intelligence in the conduct of cyber operations. If confirmed, I would be sure to continue assessing the cyber force model in light of this distinction as that model evolves.

Would you expect that military cyber operations personnel assigned to CYBERCOM units will continue to be funded mainly in the intelligence budget and compete with intelligence priorities?

If confirmed, I will likely conduct an assessment to determine the optimal methods to ensure appropriate funding for USCYBERCOM personnel.

Range Support for Cyber Command

The National Defense Authorization Act (NDAA) for Fiscal Year 2014 included a provision requiring 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. The Committee understands that the community responsible for planning and managing cyber range capabilities has developed a plan for acquiring the range capabilities that CYBERCOM requires, but has not programmed funding to implement the plan.

From your position as Deputy Assistant Secretary of Defense for Cyber Policy, how do you expect the Department will implement the NDAA legislation?

The Department is working to establish the DoD Enterprise Cyber Range Environment (DECRE) governance body to oversee Cyber Range issues. DECRE is currently working on establishing a persistent test and training environment intended to meet the demand of the Cyber Mission Force teams that are being fielded by providing on demand environments for training in both offensive and defensive cyberspace operations. The Department is also conducting an assessment to determine if we have the required cyber range capacity and capability to support Cyber Mission Force training. This assessment is expected to be completed by October 2014.

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 test and training environment is being developed based on requirements from USCYBERCOM's Exercise CYBER FLAG, and represents our current best estimate of what cyber range capabilities are needed to train the Cyber Mission Force teams. Additionally, we are assessing the capacity needed to train all of the cyber forces as they are formed and will include requirements for large-scale exercises such as CYBER FLAG, as well as National Mission Force Headquarters and Joint Force Headquarters-Cyber training, certification, and exercises.

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 is that the IAD conducts cyber protection-related duties, which fall under the responsibility of the CIO, not the USD(I).

As the position to which you have been nominated is presumed to become the principal cyber advisor to the Secretary of Defense, what are your views on the pros and cons of these proposals?

I support the President's decision to maintain the Information Assurance Directorate within NSA, as the synergy between information assurance and the signals intelligence missions should be maintained. Altering civilian relationships for oversight of the information assurance mission might risk creating divergent chains of oversight that are not synchronized with operational chains of command. However, it is undeniable that the

Chief Information Officer (CIO) has a critical role to play as well. The interaction between CIO, USD(I), and IAD is an important one, and it must be closely monitored to ensure that the current oversight structure is functioning effectively.

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 the National Security Agency (NSA) and the Commander of U.S. Cyber Command (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.

Do you support the President's decision?

I support the President's decision against separating these two positions at this time.

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?

When USCYBERCOM was established in 2009, the dual-hat arrangement allowed for the unification of leadership for organizations responsible for defending the nation in cyberspace and for signals intelligence. We continue to do extensive analysis of whether USCYBERCOM should remain a sub-unified command under USSTRATCOM or be unified to a full combatant command. We will continue to remain in close consultation with Congress if the Department believes the current arrangement should change to ensure USCYBERCOM remains operationally effective. Regardless of USCYBERCOM's potential status as a command in the future, if confirmed I will work with my colleagues throughout the Department to ensure USCYBERCOM has the resources it needs to continue to mature.

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?

In the coming years, I expect the Department will continue to closely assess

USCYBERCOM's maturation and its ability to execute its missions. This includes ensuring that USCYBERCOM has control over those assets its needs to be successful. Given NSA's status as a combat support agency, I anticipate NSA will continue to be supportive of USCYBERCOM's maturation. If confirmed, I will look forward to working with colleagues across the Department to ensure USCYBERCOM has the support it needs.

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 terminated?

I am confident that NSA will continue to provide mission-critical support to USCYBERCOM and other combatant commands, regardless of the status of the dual-hat arrangement.

Support for the Combatant Commands

The Secretary of Defense has ordered the military services and CYBERCOM to quickly 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?

As the Department builds out the Cyber Mission Force and its teams, we will continue to evaluate and evolve command and control to ensure cyber capabilities are integrated and responsive to the combatant command operations.

Have cyber operations been integrated into the operations plans of the combatant commands?

Yes, cyber capabilities are being integrated into planning the same as other capabilities from the physical domains. This is an area, however, in which the Department must continue to make steady progress.

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

Equipping the Cyber Mission Force teams is a work in progress. In addition to presenting trained personnel for the Cyber Mission Force, the Services are responsible for presenting real capability for the force. The Combat Mission Teams (CMTs), in particular, have unique requirements for full-spectrum military capabilities and the Services must continue to invest in capabilities to achieve cyber effects against DoD priority targets.

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

Though the Cyber Mission Force build is still in its infancy, today, we have National Mission Teams (NMTs) and CMTs with fully trained personnel and equipped with sufficient technical capabilities needed to conduct their missions particularly against threats in the USPACOM and USCENTCOM areas of responsibility, based on the threat. The NMTs and CMTs have very different missions and therefore require very different sets of capabilities. As the force build continues, the Department will continue to develop capabilities for the National Mission Teams, the Combat Mission Teams, as well as the Cyber Protection Teams, since defending our networks is our top priority.

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

Just as they man, train and equip for the Combatant Commanders in other domains, the Services will continue to be responsible for equipping USCYBERCOM and the Combatant Commanders with cyber capabilities to conduct their missions.

Is it your view that CYBERCOM forces would control all cyber operations regardless of target type and battlefield situation, including where cyber and traditional electronic warfare are intertwined?

I expect that control and employment of cyber operations will be in accordance with a model that will enable effective control and synchronization of cyberspace operations while balancing regional and global priorities. In regional situations where a combatant command is in the lead, USCYBERCOM will provide direct support to ensure its cyber capabilities mesh will the supported command's operations. In a global situation, U.S. STRATCOM will be the supported command and, as USSTRATCOM's operational lead for cyber, USCYBERCOM will direct the operations of regional units to ensure they are in synch with global priorities.

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 capabilities for the Cyber Mission Force. Combined, the Services and their dedicated research and development labs, DARPA, federally-funded research and development centers (FFRDCs), the defense industrial base, and the private sector all contribute greatly to providing real, viable cyber capability to the DoD. As the build of the Cyber Mission Force continues, USCYBERCOM will continue to leverage the expertise of these organizations to build diverse capability to enable full-spectrum military operations.

In October 2013, the Department made a series of decisions to 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.

Cyber Personnel

The military services have already provided thousands of service members to man cyber mission units assigned to CYBERCOM. These personnel are going through training provided by the NSA. CYBERCOM, working with the services, NSA, and others, has developed position descriptions, roles, and skills, and training programs. Over the next couple of years, the services will be identifying thousands more positions for additional units before the current force goals are met.

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

The Services have some personnel with existing cyber skills. The Department is working to determine and grant, as appropriate, training equivalencies for these qualified personnel assigned to the cyber mission forces. For future personnel, the Services are applying screening criteria to ensure those entering training programs have the skills and aptitude to succeed. The Services are employing recruiting and retention mechanisms to facilitate the build plan for the cyber mission forces, including those specifically meeting USCYBERCOM's needs.

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?

This has been a priority for DoD's senior leadership, and the subject of recent senior-level decision forums over the past year. As a result of guidance from the Deputy Secretary of Defense, each Service provided assessments of their ability to meet USCYBERCOM training requirements, and the Joint Staff has been closely tracking progress across the range of readiness categories, including training. There has been significant progress by each Service in meeting the training goals, but because this is a multi-year effort, we don't expect to see full maturation across the Cyber Mission Force until FY 2016.

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?

As a result of recent senior DoD decision management processes, each Service was given direction to prioritize the establishment of personnel management mechanisms to identify, recruit, retain, and provide incentivized career advancement paths for both military and civilian personnel with the type of high-end, advanced operational skills that USCYBERCOM has identified within the Cyber Mission Force. There has been steady progress by each Service toward meeting this guidance, and this issue continues to be followed closely in monthly reporting by USCYBERCOM to the Joint Staff. One of the more significant challenges in implementing the guidance has been in the civilian workforce, where DoD is looking at options that may require the assistance of Congress.

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?

If confirmed, I would work with Congress, the Military Departments, and the Services to examine where the potential delegation of personnel authorities might be appropriate for consideration to maximize USCYBERCOM's mission effectiveness as it evolves.

Relationship with U.S. Northern Command

U.S. Northern Command was established in October 2002 with the mission of conducting operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the Command's assigned area of responsibility; and, as directed by the President or Secretary of Defense, to provide military assistance to civil authorities, including consequence management operations.

If confirmed, how do you anticipate you would coordinate roles and responsibilities with the Commander of U.S. Northern Command?

If confirmed, I would expect to work closely with the Commander of U.S. Northern Command (USNORTHCOM) to support the efforts of the Secretary of Defense on the broad array of issues touching on homeland defense, Defense Support of Civil Authorities, theater strategy and policy, contingency planning, and policy oversight of operations.

How do you anticipate that the Assistant Secretary of Defense for Homeland Defense and the Commander of U.S. Northern Command will coordinate with other federal and State entities in planning for response to catastrophic events that might require Defense Department support?

If confirmed, I look forward to working closely with the Commander of USNORTHCOM to ensure that DoD support to Federal and State entities in response to catastrophic events, if required, is provided in a timely and coordinated fashion. It is my understanding that this begins with DoD positioning itself to support civil authorities during disaster response activities by building its own resilience against cascading failures of critical infrastructure. Moreover, this effort continues, through the Secretary's complex catastrophe initiative, to ensure that the Department is able to provide its civil support capabilities from all components in support of civil authorities, making defense support of civil authorities faster and more effective when delivering life-saving and life-sustaining requirements.

Partnership with the National Guard and the States

The Department of Defense has an important partnership with the National Guard because it has both federal and state responsibilities. The Department has worked with the Council of Governors to establish procedures to ensure unity of effort between military forces operating in federal and state status, including the creation of "dual-status commanders."

Please summarize your understanding of how this unity of effort is maintained through the dual status commander arrangement, so that the authorities of the President and Secretary of Defense are preserved for federal military forces, and the authorities of Governors are preserved for National Guard forces acting in a state capacity.

As I understand it, a signed memorandum of agreement between a Governor and the Secretary of Defense provides the terms, responsibilities, and procedures for the use of a dual-status commander, including the procedures for preserving the separate and

mutually exclusive Federal and State chains of command. These procedures are tested in annual exercises and used in real-world operations such as the response to Super Storm Sandy in 2012.

National Guard and Reserve Role in Homeland Defense

The ASD for Homeland Defense has policy responsibility for the participation of National Guard units or personnel in homeland defense activities, when the Secretary of Defense determines that such participation is necessary and appropriate.

What role do you believe the National Guard and Reserves should have in homeland defense, and how does their role relate to the role of the Active Component?

I believe that homeland defense is viewed as a Total Force Mission. The role of the National Guard and non-National Guard Reserve forces is to integrate with Active Component forces seamlessly to accomplish U.S. objectives. National Guard and non-National Guard Reserve units are organized, trained, and equipped to succeed in accomplishing assigned missions.

What role do you believe the National Guard and Reserves should have in providing civil support assistance to other federal agencies, and how does their role relate to the role of the Active Component?

Civil Support – or "Defense Support of Civil Authorities" as DoD terms it – is a Total Force responsibility. All of the appropriate resources of the Department, including those of the various Defense Agencies, are integrated in support of other Federal departments and agencies for specific missions. With the recent authority provided in the National Defense Authorization Act for Fiscal Year 2012, non-National Guard Reserve forces may now be activated to provide assistance to respond to Federal requests during responses to major disasters and emergencies.

Use of Active Duty and Reserve Personnel for Homeland Defense/Posse Comitatus

What is your understanding of the legal issues and authority associated with using National Guard and Reserve personnel in security roles within the United States?

Under the authority of state Governors, in State active duty status or duty status under title 32, the National Guard is not subject to the restrictions imposed by the Posse Comitatus Act. However, when ordered to active duty, National Guard and non-National Guard Reserve forces are subject to the restrictions imposed by the Posse Comitatus Act and DoD policy.

The National Guard, as a State militia, under the command and control of respective

Governors and Adjutants Generals, may be used for any security role authorized under State law. When the Reserve Components (including the National Guard) are mobilized under title 10, and placed under Federal command and control, they are subject to the same restrictions as other Federal military forces.

In your opinion, does the Posse Comitatus Act (18 U.S.C. § 1385) or chapter 18 of title 10, U.S.C. (which regulates the use of the armed forces in support of civilian law enforcement and related activities) require amendment to deal with the present homeland security situation?

No. I believe that current laws and policies governing DoD's role in support to civilian law enforcement-related activities are sufficient.

Under what circumstances do you believe that it is appropriate for the Department of Defense to provide assistance to law enforcement authorities in response to a domestic terrorist event? What about a non-terrorist event?

As I understand it (under title 18, U.S. Code, Section 831), the U.S. Attorney General may request that the Secretary of Defense provide emergency assistance if an emergency situation exists in which civilian law enforcement personnel are not capable of enforcing the law to address certain types of threats involving nuclear materials, such as potential use of a nuclear or radiological weapon. This could be for either a domestic terrorist event or a non-terrorist event.

The Department does provide non-direct support to civilian law enforcement on a routine basis. As an example, DoD provides subject matter experts in the area of explosive ordnance disposal to detect and, if necessary, render safe an improvised explosive device that is of military origin. Further, DoD can provide logistics and training assistance to civilian law enforcement authorities.

In response to a domestic terrorist event, I believe it is appropriate to provide DoD assistance to law enforcement authorities under existing authorities when requested by the U.S. Attorney General or directed by the President of the United States.

For non-terrorist events, DoD does provide assistance to law enforcement authorities, consistent with the Posse Comitatus Act and other restrictions, to save human lives, mitigate human suffering, and prevent wide-spread property damage.

If confirmed, what role do you expect to play in making such determinations and making such assistance available?

If confirmed, I would be the principal civilian advisor to the Secretary of Defense under the USD(P) on all matters related to Defense Support of Civilian Authorities. I expect

that this would include support to civilian law enforcement agencies by DoD where appropriate. If confirmed, I would work with others in the Office of the Secretary of Defense, the Joint Staff, and heads of the DoD Components and activities to facilitate informed decision-making by the Secretary of Defense.

Policy to Counter Weapons of Mass Destruction

The plan to reorganize the Office of the Under Secretary of Defense for Policy envisions the ASD for Homeland Defense having primary policy and oversight responsibility for countering weapons of Mass Destruction (WMD), meaning nuclear, biological, and chemical weapons. This would be a new responsibility for the ASD for Homeland Defense.

Please describe your understanding of the programs and activities to counter WMD for which the ASD for Homeland Defense would have policy responsibility.

I understand that, in the future, the Assistant Secretary of Defense for Homeland Defense will be responsible for developing strategies and policies, and overseeing the execution of approved policies and programs, including chemical, biological, radiological, and nuclear (CBRN) defense; WMD and missile-related proliferation; and Cooperative Threat Reduction (CTR) program activities.

What do you believe are the principal challenges in countering Weapons of Mass Destruction and, if confirmed, what would be your priorities for Department of Defense policy for countering WMD?

Preventing the proliferation or use of weapons of mass destruction by either State or terrorist actors is our principal challenge. The ability to respond to and mitigate WMD attacks remains essential, but our homeland, citizens, and interests are best protected by ensuring that these threats never fully materialize. I believe that by reducing incentives to proliferation, increasing the barriers to acquisition and use, and denying the effects of current and emerging WMD threats we can better protect our citizens and interests at home and abroad. If confirmed, I would prioritize DoD's efforts in these areas.

If confirmed, what role do you expect to play in the creation of policy for, and oversight of, Defense Department programs to counter Weapons of Mass Destruction, and how would you ensure effective policy coordination of the various DOD actors and programs to counter WMD?

If confirmed, my office would play a lead role in developing policies to prevent and counter WMD threats to our interests and citizens at home and abroad. This includes guiding Defense Department efforts to protect and defend our forces from such threats, bolstering the capabilities of allies and partners to deal with these challenges, ensuring appropriate support to civil authorities should these weapons threaten us at home, and

developing the strategies, plans, and capabilities for DoD to prevent and mitigate these risks overseas. Countering WMD is a whole-of-government effort, and, if confirmed, I expect to partner with DoD, interagency, and international partners to ensure that appropriate policy and oversight are in place to reduce these threats and protect our interests.

Cooperative Threat Reduction Program

If confirmed, what will your role be in implementing and overseeing the Cooperative Threat Reduction (CTR) Program?

If confirmed, I would continue the role currently performed by the ASD for Global Security Affairs (ASD (GSA)) as that responsibility migrates to the Office of the Assistant Secretary of Defense for Homeland Defense. I would provide policy guidance to the director of the Defense Threat Reduction Agency for implementing the CTR Program and continue to coordinate with the ASD/NCB on program implementation issues.

If confirmed, what changes, if any, would you recommend to the CTR program, including changes in legislative authorities, programs, or funding?

My understanding is that the DoD CTR Program has had, for the most part, the authorities, programs, and funding needed to address emerging WMD threats appropriately. Most of the DoD CTR legislation has existed for about twenty years, and therefore, if confirmed, I would work with interagency partners and Congress to review the existing legislation to see if it requires updating.

How do you envision the evolution of the program as it transitions away from Russia to countries outside the former Soviet Union?

WMD threats are global, and I envision that the CTR Program will continue to evolve to meet those threats. I understand that the CTR Program is focused on countering WMD terrorism threats. If confirmed, I would work to ensure that CTR is well-positioned to continue to address those threats while also responding to unique challenges such as those posed by chemical weapons stockpiles in Libya and Syria, in cooperation with U.S. Government and international partners.

Chemical and Biological Defense

One of the issue areas that will be placed under the Assistant Secretary of Defense for Homeland Defense is the Chemical and Biological Defense Program of the Defense Department.

What do you believe are the principal challenges in chemical and biological defense, and what would be your priorities for the DOD Chemical and Biological Defense Program?

As part of the Department's overall effort to counter WMD, the Office of the ASD/NCB manages the Chemical and Biological Defense (CBD) Program. I understand that the ASD for Homeland Defense would be responsible for development of policies to guide the program and would work to ensure close coordination between our offices. If confirmed, I would work to ensure that, given the constrained fiscal environment, the Department prioritizes capabilities that counter operationally significant risks, taking into consideration potential contributions from other partners in the U.S. Government or the international community.

Do you believe the Chemical and Biological Defense Program should be closely coordinated with related efforts of the Defense Department's Cooperative Threat Reduction program focused on reducing biological threats?

The President has highlighted the importance of countering biological threats, and my understanding is that both the CBD and CTR Programs strongly support this priority. I agree with these priorities, and if confirmed, would work to ensure awareness of and close coordination between the two Programs.

Do you believe the Chemical and Biological Defense Program should be coordinated closely with the Department of Health and Human Services in their respective development of medical countermeasures against chemical, biological, and radiological hazards?

Yes, I believe that close coordination of the Department and HHS medical countermeasure efforts is required. I understand that both Departments are currently working together to ensure respective medical countermeasure efforts are transparent and mutually supportive, and if confirmed, I would continue this close coordination.

Chemical Demilitarization

DOD Directive 5160.05E states the DOD policy that "the Department of Defense shall be in full compliance" with the Chemical Weapons Convention (CWC) and the Biological Warfare Convention (BWC). In 2006, the Department announced that the United States would not meet even the extended deadline of April 2012 for destruction of its chemical weapons stockpile, as required under the CWC, and the United States does not expect to complete destruction until after 2020.

Do you agree that the Department of Defense and the United States Government should be in full compliance with the terms and obligations of the CWC and the BWC, including the deadline for destruction of the U.S. chemical weapons stockpile under the CWC?

I understand that in 2006 the United States informed the Organization for the Prohibition of Chemical Weapons (OPCW) that it did not expect to meet the 2012 CWC deadline for

complete destruction of the U.S. chemical weapons stockpile. Since then, the United States has continued to follow a policy of transparency about the U.S. chemical weapons destruction program and has stressed U.S. efforts to complete chemical weapons destruction as safely and quickly as practicable. If confirmed, I would continue to support a policy of transparency and would support continued efforts to destroy the remainder of the U.S. chemical weapons stockpile as safely and quickly as practicable.

If confirmed, will you work to ensure that the Department takes steps needed to minimize the time to complete destruction of the U.S. chemical weapons stockpile, without sacrificing safety or security, and that the Department requests the resources necessary to complete destruction as close to the deadline as practicable?

The Office of the USD (AT&L) and the Department of the Army continue to focus significant senior leadership attention on completing destruction of the U.S. chemical weapons stockpile as safely and quickly and practicable. If confirmed, I would work closely with these offices to ensure continued focus on meeting this objective.

Proliferation Security Initiative

The Proliferation Security Initiative (PSI) is an international effort to identify and interdict weapons of mass destruction and related materials.

If confirmed, would you recommend that the PSI program continue and, if so, do you believe that it should be modified in any way?

I support the Proliferation Security Initiative and, if confirmed, would work to implement President Obama's call to make PSI a more durable effort. PSI has led the way in building international consensus on the importance of countering proliferation-related shipments. I believe that PSI sends a strong deterrent message to proliferators, strengthens nonproliferation engagement with partners, and builds partner capacity to interdict illicit WMD-related shipments.

Defense Space Policy

The plan to reorganize the Office of the Under Secretary of Defense for Policy envisions the ASD for Homeland Defense having primary responsibility for DOD Space policy. This would be a new responsibility for the ASD for Homeland Defense.

Please describe your understanding of the space policy responsibilities intended for the ASD for Homeland Defense, and how those responsibilities would relate to cyber security policy responsibilities.

As I understand it, under the plan to reorganize the Office of the USD(P), the Space Policy

functions will be overseen by a Deputy Assistant Secretary of Defense (DASD) responsible for Space and Cyberspace, who will report to the Assistant Secretary of Defense for Homeland Defense. In my previous experience as the DASD for Cyber Policy, I worked closely with the DASD for Space Policy and we reported to the same Assistant Secretary, so the reorganization would maintain the close alignment between these two offices. These days, cyber and space policy face similar challenges. If confirmed, I would continue the close collaboration between these two critical areas. I would also participate actively in the development and oversight of space policy and strategy for the Department, in the DoD space-related decision-making processes, and in the DoD Planning, Programming, Budgeting, and Execution (PPBE) processes to ensure space system architectures support our national security objectives effectively.

If confirmed, what would be your priorities for Department of Defense policy for space, and how would you ensure effective execution of DOD space policy?

If confirmed, I would place priority on U.S. space control capability and on increasing national security space resiliency against growing threats to space-based architectures. Both Presidential and DoD guidance directs the Department to retain counter-space capabilities to address the growing space capabilities of potential adversaries, including anti-satellite capabilities. Through partnerships with commercial suppliers, collaboration with international partners, and changes in our own architectures and operational tactics, we can improve the resiliency of our systems and strengthen strategic stability in space.

If confirmed, what role will you play in establishing architectures for various space systems, such as those for communications and Overhead Persistent Infra-red (OPIR)?

If confirmed, I would participate actively in the development of space architectures and the Planning, Programming, Budgeting, and Execution (PPBE) processes of the Department to ensure space system architectures support our national security objectives effectively, including our National Security Space Strategy.

If confirmed, what role will you play in developing a space protection strategy, and working with U.S. STRATCOM to implement that strategy, such as improving space situational awareness?

If confirmed, I would work closely with the Commander, U.S. Strategic Command, to ensure appropriate and effective strategies are in place to increase our space situational awareness and to ensure that critical space capabilities are resilient and redundant, in order to maintain the advantages provided by these capabilities. I believe that continually improving space situational awareness underpins our ability to operate safely in the increasingly congested and contested space environment and enables the protection of our space assets. In addition, if confirmed, I would look to partner with the Space

Security and Defense Program (SSDP) and the efforts they have been undertaking to develop a space protection strategy.

Over the course of the last several years there has been discussion about establishing international space rules of the road to deal with, mitigate, and reduce the generation of space debris.

What are your views on establishing space rules of the road?

Establishing non-legally binding norms for the responsible, peaceful, and safe use of space and preservation of the space environment is an important issue for all space-faring nations. Pragmatic guidelines, or rules of the road, could help avoid collisions and other debris-generating events, reduce radiofrequency interference, and strengthen safety, stability, sustainability, transparency, and security in the space domain. If confirmed, I would work to ensure that development of international norms strengthens safety and sustainability in space, consistent with U.S. national security interests.

Space Posture Review

If confirmed, what role will you play in overseeing and implementing the policies, strategies, and priorities established in the Space Posture Review?

If confirmed, I would support the USD(P) and the Secretary as they continue to implement the President's 2010 National Space Policy and the National Security Space Strategy, which included the Space Posture Review. I would help to develop and oversee implementation of DoD's space-related policies, and oversee implementation of strategy and plans related to space forces, systems, and activities in close coordination with other DoD officials, including by serving on the Defense Space Council.

Terrorist Threat to the Homeland

In your view, what is the extent of the current threat to the Homeland of terrorist extremists both from outside the United States and from within the United States?

Based on my understanding of intelligence community judgments, there is no question that al Qaeda, its associates, affiliates, and adherents continue to maintain the intent to strike the United States, posing a persistent threat to the homeland. A relatively new phenomenon is the growth of homegrown violent extremists (HVEs) who are motivated by al Qaeda ideology to conduct attacks in the homeland. The intelligence community assesses judges that the number one target of HVEs is DoD installations and facilities. Al Qaeda, its associates, affiliates, and adherents continue to produce English-language propaganda that inspires and encourages violent attacks, highlighting al Qaeda's de-centralized nature since there is no direct command and control over the plotting or

conduct of this type of attack.

How would you broadly characterize that threat – low, medium, or high?

I would characterize the threat as persistent. There are threat streams that at the time of receiving them run the range of threat from low to high. Al Qaeda, its associates, affiliates, and adherents publicly express and maintain the intent to attack the homeland, and they are constantly seeking the best capability to do so. If confirmed, I look forward to working closely with the Intelligence Community to help to prevent an attack against the United States.

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 in a timely manner.

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

Yes. If confirmed, I would appear before the congressional defense committees or other appropriate committees on matters under the purview of the Assistant Secretary of Defense for Homeland Defense.

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 the Assistant Secretary of Defense for Homeland Defense?

Yes. If confirmed, I would appear and provide information to this committee, or its designated membership, on matters under the purview of the Assistant Secretary of Defense for Homeland Defense.

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. If confirmed, I agree to provide information to this committee and its staff on matters under the purview of the Assistant Secretary of Defense for Homeland Defense.

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. If confirmed, I would provide documents subject to appropriate and necessary security protection.