STATEMENT OF

GENERAL KEITH B. ALEXANDER

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

SENATE COMMITTEE ON ARMED SERVICES

12 MARCH 2013

Thank you very much Chairman Levin and Ranking Member Inhofe for inviting me to speak to you and your colleagues today on behalf of the men and women of U.S. Cyber Command. I have the honor of leading them on a daily basis, and let me assure you there is not a finer and more dedicated team of Service members and civilian personnel anywhere. It gives me great pleasure to appear before you to talk about their accomplishments, and to describe some of the challenges they face in performing their difficult but vital mission of keeping U.S. military networks secure, helping to protect our nation's critical infrastructure from national-level cyber attacks, assisting our Combatant Commanders around the world, and working with other U.S. Government agencies tasked with defending our nation's interests in cyberspace.

USCYBERCOM is a subunified command of U.S. Strategic Command in Omaha, though we are based at Fort Meade, Maryland. We have approximately 834 active-duty military and civilians assigned from an authorized end-strength of 917 (plus contractors), and a budget of approximately $191 million for Fiscal Year 2013. USCYBERCOM has strong, evolving, and growing cyber components representing each of the Services: Fleet Cyber Command/Tenth Fleet, Army Cyber Command/Second Army, Air Force Cyber Command/24th Air Force, and Marine Forces Cyber Command. Each of our Service Cyber Components also has representation at our headquarters. Combined we and they have more than 11,000 people in our force mix.

US Cyber Command shares its headquarters with key mission partners in the National Security Agency (NSA), which I also lead. USCYBERCOM's co-location with NSA promotes intense and mutually beneficial collaboration. The Department of Defense established U.S. Cyber Command in 2010 to leverage NSA's capabilities. This partnership is key to what we are doing now, and provides the essential context for all the activities I shall describe below. The people under my command and direction at USCYBERCOM and NSA are collectively responsible for operating the Department's information networks, detecting threats in foreign cyberspace, attributing threats, securing national security and military information systems, and helping to ensure freedom of action for the United States military and its allies in cyberspace—and, when directed, defending the nation against a cyber attack. Also nearby at Fort Meade is another key mission partner, the Defense Information Systems Agency (DISA). The constellation of agencies and capabilities in the Washington DC region makes for a unique synergy of people and ideas—a nexus for military and national cybersecurity innovation.

USCYBERCOM has deployed representatives and mission support elements worldwide. We have an expeditionary cyber support unit forward in Afghanistan. We also have liaison officers at each Combatant Command

(serving as that Command's CSE lead) and in several other key offices and agencies in the Washington area. The flow of information and advice across USCYBERCOM and its Service components and the commands, agencies, and foreign mission partners here and overseas is improving slowly but steadily.

Since I last spoke with you in March 2012, our progress has accelerated. In December we moved ahead with building a balanced and highly capable military cyber force designed to meet our joint warfighting requirements. We have laid out and codified team composition, training, and certification standards to field a world-class force in support of the Combatant Commands (CCMDs). Although we have much work to do, we are focused on doing it right and meeting the CCMDs' and the nation's most pressing cyber defense requirements. In short, we have moved ahead to normalize cyber operations within the U.S. military, and to turn that capability into a reliable option for decisionmakers to employ in defending our nation. This progress will not only make our military more capable but our networks and information more secure. We have serious threats facing us, as I shall explain. Our progress, however, can only continue if we are able to fulfill our urgent requirement for sufficient trained, certified, and ready forces to defend U.S. national interests in cyberspace.

The Strategic Landscape

U.S. Cyber Command operates in a dynamic and contested environment that literally changes its characteristics each time someone powers on a networked device. Geographic boundaries are perhaps less evident in cyberspace, but every server, fiber-optic line, cell tower, thumb drive, router, and laptop is owned by someone and resides in some physical locale. In this way cyberspace resembles the land domain—it is all owned, and it can be re-shaped. Most networked devices, for example, are in private hands, and their owners can deny or facilitate others' cyber operations by how they manage and maintain their networks and devices. Cyberspace as an operating environment also has aspects unique to it. Events in cyberspace can seem to happen instantaneously. Data can appear to reside in multiple locations. There is a great deal of anonymity, and strongly encrypted data are virtually unreadable. In cyberspace, moreover, sweeping effects can be precipitated by states, enterprises, and individuals, with the added nuance that such cyber actors can be very difficult to identify. The cyber landscape also changes rapidly with the connection of new devices and bandwidth, and with the spread of strong encryption and mobile devices. Despite the unique characteristics of cyberspace, states still matter because they can affect much of the physical infrastructure within their borders. Convergence is our watchword; our communications, computers, and networks are merging into one digital environment as our political, economic, and social realms are being re-shaped by the rush of innovation.

In this environment that is both orderly and chaotic, beneficial and perilous, we at USCYBERCOM have to focus on actors who possess the capability—and possibly the intent—to harm our nation's interests in cyberspace or to use cyber means to inflict harm on us in other ways. Unfortunately, the roster of actors of concern to us is growing longer and growing also in terms of the variety and sophistication of the ways they can affect our operations and security.

State actors continue to top our list of concerns. We feel confident that foreign leaders believe that a devastating attack on the critical infrastructure and population of the United States by cyber means would be correctly traced back to its source and elicit a prompt and proportionate response. Nonetheless, it is possible that some future regime or cyber actor could misjudge the impact and the certainty of our resolve.

We have some confidence in our ability to deter major state-on-state attacks in cyberspace but we are not deterring the seemingly low-level harassment of private and public sites, property, and data. As former Secretary of Defense Panetta explained to an audience in New York last October, states and extremist groups are behaving recklessly and aggressively in the cyber environment. Such attacks have been destructive to both data and property. The Secretary mentioned, for example, the remote assaults last summer on Saudi Aramco and RasGas, which together rendered inoperable—and effectively destroyed the data on—more than 30,000 computers. We have also seen repressive regimes, desperate to hold on to power in the face of popular resistance, resort to all manner of cyber harassment on both their opponents and their own citizens caught in the crossfire. Offensive cyber programs and capabilities are growing, evolving, and spreading before our eyes; we believe it is only a matter of time before the sort of sophisticated tools developed by well-funded state actors find their way to non-state groups or even individuals. The United States has already become a target. Networks and websites owned by Americans and located here have endured intentional, state-sponsored attacks, and some have incurred damage and disruption because they happened to be along the route to another state's overseas targets.

Let me draw your attention to another very serious threat to U.S. interests. The systematic cyber exploitation of American companies, enterprises, and their intellectual property continued unabated over the last year. Many incidents were perpetrated by organized cybercriminals. Identity and data theft are now big business, netting their practitioners large profits and giving rise to an on-line sub-culture of markets for stolen data and cyber tools for stealing more. Much cyber exploitation activity, however, is state-sponsored. Foreign government-directed cyber collection personnel, tools, and organizations are targeting the data of American and western businesses, institutions, and citizens. They are particularly targeting our

telecommunications, information technology, financial, security, and energy sectors. They are exploiting these targets on a scale amounting to the greatest unwilling transfer of wealth in history. States and cybercriminals do not leave empty bank vaults and file drawers behind after they break-in—they usually copy what they find and leave the original data intact—but the damage they are doing to America's economic competitiveness and innovation edge is profound, translating into missed opportunities for U.S. companies and the potential for lost American jobs. Cyber-enabled theft jeopardizes our economic growth. We at USCYBERCOM work closely with our interagency partners to address these threats.

We must also watch potential threats from terrorists and hacktivists in cyberspace. The Intelligence Community and others have long warned that worldwide terrorist organizations like al Qaeda and its affiliates have the intent to harm the United States via cyber means. We agree with this judgment, while noting that, so far, their capability to do so has not matched their intent. This is not to downplay the problem of terrorist use of the Internet. Al Qaeda and other violent extremist groups are on the Web proselytizing, fundraising, and inspiring imitators. We should not ignore the effectiveness with which groups like al Qaeda and its affiliates radicalize ever larger numbers of people each year—on more continents. The Federal Bureau of Investigation and other agencies cite instances in which would-be terrorists found motivation and moral support for suicide attacks at jihadist websites and chat rooms. This is an especially serious and growing problem in areas of hostilities where our troops and personnel are deployed. Another threat that is not growing as fast as we might have feared, on the other hand, is that of hacktivists with a cause or a grievance that leads them to target U.S. government and military networks. Our vulnerabilities to this sort of disruption remain, but 2012 saw fewer such incidents than 2011.

Looking Ahead: The Command's Priorities

I have established several priorities for U.S. Cyber Command in dealing with these risks and threats. We are actively working to guard the Department of Defense's networks and information and helping to defend the nation. Key to countering these threats is learning <u>how</u> to grow our capabilities in this challenging domain. We have no alternative but to do so because every world event, crisis, and trend now has a cyber-aspect to it, and decisions we make in cyberspace will routinely affect our physical or conventional activities and capabilities as well. USCYBERCOM is building cyber capabilities into our planning, doctrine, and thinking now—while we as a nation have time to do so in a deliberate manner. We do not want to wait for a crisis and then have to respond with hasty and ad hoc solutions that could do more harm than good.

When I say we are normalizing cyber operations, I mean we are making them a more reliable and predictable capability to be employed by our senior decisionmakers and Combatant Commanders. Normalizing cyber requires improving our tactics, techniques, and procedures, as well as our policies and organizations. It also means building cyber capabilities into doctrine, plans, and training – and building that system in such a way that our Combatant Commanders can think, plan, and integrate cyber capabilities as they would capabilities in the air, land and sea domains.

In keeping with the Department of Defense's *Strategy for Operating in Cyberspace*, U.S. Cyber Command and NSA are together assisting the Department in building: 1) a defensible architecture; 2) global situational awareness and a common operating picture; 3) a concept for operating in cyberspace; 4) trained and ready cyber forces; and 5) capacity to take action when authorized. Indeed, we are finding that our progress in each of these five areas benefits our efforts in the rest. We are also finding the converse—that inertia in one area can result in slower progress in others. I shall discuss each of these priorities in turn.

Defensible Architecture: The Department of Defense (DoD) owns seven million networked devices and thousands of enclaves. Cyber Command works around the clock with its Service cyber components, with NSA, and with DISA to monitor the functioning of DoD networks, including the physical infrastructure, the configurations and protocols of the components linked by that infrastructure, and the volume and characteristics of the data flow. This is a dynamic defense, and it consistently provides better security than the former patch-and-firewall paradigm. Patches and firewalls are still necessary—I wish everyone kept theirs up-to-date—but they are an insufficient defense for DoD networks. Dynamic defenses have brought about noticeable improvements in the overall security of DoD information environment. We know for a fact that our adversaries have to work harder to find ways into our sensitive but unclassified networks. Unfortunately, adversaries are willing to expend that effort, and DoD's architecture in its present state is not defensible over the long run. We in the Department and the Command are crafting a solution. The Department's bridge to the future is called the DoD Joint Information Environment (JIE), comprising a shared infrastructure, enterprise services, and a single security architecture to improve mission effectiveness, increase security, and realize information technology (IT) efficiencies. The JIE will be the base from which we can operate in the knowledge that our data are safe from adversaries. Senior officers from USCYBERCOM and NSA sit on JIE councils and working groups, playing a leading role with the office of the DoD's Chief Information Officer, Joint Staff J6, and other agencies in guiding the Department's implementation of the JIE. NSA, as the Security Adviser to the JIE, is defining the security dimension of that architecture, and has shown how we can pool big data and still preserve strong security. We have even shared the source code publicly so public and private architectures can benefit

from it. DoD is benefitting from that knowledge and from our growing understanding of the totality of measures, procedures, and tools required to assure the health and security of even the biggest networks and databases.

Increased Operational Awareness: Enhanced intelligence and situational awareness in our networks will help us know what is happening in the cyberspace domain. This effort can be likened to a cyber version of the tactical air picture of friendly, neutral, and aggressor aircraft that a Combined Air Operations Center in a Combatant Command typically maintains. We are now issuing a weekly Cyber Operating Directive (CyOD) across the DoD cyber enterprise for just this purpose, so that all "friendlies" understand what is happening in cyberspace. Our improving knowledge of what is normal in cyberspace is crucial to grasping what is not normal. We at USCYBERCOM are also helping DoD increase our global situational awareness through our growing collaboration with federal government mission partners like the Department of Homeland Security (DHS), the FBI, and other departments and agencies, as well as with private industry and with other countries. That collaboration in turn allows us to better understand what is happening across the cyber domain, which enhances our situational awareness, not only for the activities of organizations based at Fort Meade but also across the U.S. government. I am happy to report that at least one of our foreign partners has volunteered to invest in this and enter its own network traffic data to contribute to a common picture.

Operating Concepts: Our operating concept calls for us to utilize our situational awareness to recognize when an adversary is attacking, to block malicious traffic that threatens our networks and data, and then to maneuver in cyberspace to block and deter new threats. I am pleased to report that in December, the Department endorsed the force presentation model we need to implement this new operating concept. We are establishing cyber mission teams in line with the principles of task organizing for the joint force. The Services are building these teams to present to U.S. Cyber Command or to support Service and other Combatant Command missions. The teams are analogous to battalions in the Army and Marine Corps—or squadrons in the Navy and Air Force. In short, they will soon be capable of operating on their own, with a range of operational and intelligence skill sets, as well as a mix of military and civilian personnel. They will also have appropriate authorities under order from the Secretary of Defense and from my capacity as the Director of NSA. Teams are now being constructed to perform all three of the missions given to U.S. Cyber Command. We will have 1) a Cyber National Mission Force and teams to help defend the nation against national-level threats; 2) a Cyber Combat Mission Force with teams that will be assigned to the operational control of individual Combatant Commanders to support their objectives (pending resolution of the cyber command and control model by the Joint Staff); and 3) a Cyber Protection Force and teams to help operate and defend DoD information environment.

Trained and Ready Forces: Each of these cyber mission teams is being trained to common and strict operating standards so that they can be on-line without putting at risk our own military, diplomatic, or intelligence interests. Doing this will give not only U.S. Cyber Command's planners, but more significantly our national leaders and Combatant Commanders, a certain predictability in cyber capabilities and capacity. Key to building out the Cyber Mission Force articulated in our Force Planning Model is having the training system in place to train each of the cyber warriors we need, in the skill sets we require and at the quality mandated by the cyber mission. We have that training system in place for the operators, and now we need to build the accompanying Command and Staff academic support packages and programs to ensure our officers and planners know how to effectively plan for and employ cyber capabilities for our nation. As a result of this operator and staff training system, decisionmakers who require increments of cyber skills to include in their plans will know how to ask for forces to fill this requirement, and planners will know how to work cyber effects into their organizations' plans. To build the skills of the force—as well as to test the ways in which its teams can be employed—U.S. Cyber Command has sponsored not only an expanding range of training courses but also two important exercises, CYBER FLAG and CYBER GUARD. The latter assembled 500 participants last summer including a hundred from the National Guards of twelve states. They exercised state and national-level responses in a virtual environment, learning each other's comparative strengths and concerns should an adversary attack our critical infrastructure in cyberspace. CYBER FLAG is our annual exercise at Nellis Air Force Base in Nevada and we conduct it with our inter-agency and international partners. Our most recent running of CYBER FLAG introduced new capabilities to enable dynamic and interactive force-on-force maneuvers at net-speed, while incorporating actions by conventional forces as well at Nellis' nearby training area.

Capacity to Take Action: Successful operations in cyberspace depend on collaboration between defenders and operators. Those who secure and defend must synchronize with those who operate, and their collaboration must be informed by up-to-date intelligence. I see greater understanding of the importance of this synergy across the Department and the government. The President recently clarified the responsibilities for various organizations and capabilities operating in cyberspace, revising the procedures we employ for ensuring that we act in a coordinated and mutually-supporting manner. As part of this progress, the Department of Defense and U.S. Cyber Command are being integrated in the machinery for National Event responses so that a cyber incident of national significance can elicit a fast and effective response to include pre-designated authorities and self-defense actions where necessary and appropriate. USCYBERCOM is also working with the Joint Staff and the Combatant Commands to capture their cyber requirements and to implement and refine interim guidance on the command and control of cyber forces in-

theater, ensuring our cyber forces provide direct and effective support to commanders' missions while also helping U.S. Cyber Command in its national-level missions. In addition, we are integrating our efforts and plans with Combatant Command operational plans and we want to ensure that this collaboration continues at all the Commands. Finally, most cyber operations are coalition and interagency efforts, almost by definition. We gain valuable insight from the great work of other partners like the Departments of Justice and Homeland Security, such as in their work against distributed denial of service attacks against American companies, which in turn helps DoD fine-tune defenses for the DoD information environment. We also benefit from sharing with the services and agencies of key partners and allies. We welcome the interagency collaboration and evolving frameworks under which these efforts are proceeding, especially such revisions that would make it easier for the U.S. Government and the private sector to share threat data, as the administration previously emphasized. In addition, new standing rules of engagement for cyber currently under development will comply with and support recently issued policy directives on U.S. cyber operations.

Building for the Future

We have made strides in all of our focus areas, though what gratifies me the most is seeing that we are learning how they all fit together. We are building quickly and building well, but we are still concerned that the cyber threats to our nation are growing even faster. From the technological, legal, and operational standpoints we are learning not only what is possible to accomplish but also what is wise to attempt. Our plans for U.S. Cyber Command over the foreseeable future—which admittedly is not a very distant horizon—should be understood in this context.

In a speech last fall, then-Secretary Panetta emphasized the Department's need to adjust our forces as we transition away from a decade of war. He explained that a wise adjustment makes cuts without hollowing out the force, while also investing in ways that prepare us to meet future needs. We will do that, he said, by increasing our investments in areas including space and cyber. It is fair to ask how we plan to use such new resources while others are trimming back. Our new operating concept to normalize cyber capabilities is just the sort of overarching theme to unite the whole institutional push. We need to foster a common approach to force development and force presentation—up to and including the Service component and joint headquarters—given the intrinsically joint nature of this domain.

Let me emphasize that this is not a matter of resources alone – it is a matter of earning trust. We will continue to do our work in full support and defense of the civil liberties and privacy rights enshrined in the U.S.

Constitution. We do not see a tradeoff between security and liberty. We can and must promote both simultaneously because each enhances the other. U.S. Cyber Command takes this responsibility very seriously. Indeed, we see this commitment in our day-by-day successes. We in the Department of Defense and DHS, with DOJ and industry, for instance, have shown that together we can share threat information, to include malware signatures, while still providing robust protection for privacy and civil liberties..

Building the Department's defensible cyber architecture will let us guard our weapons systems and military command and control as well as our intelligence networks. We hope to take the savings in personnel and resources gained by moving to the JIE and have the Services repurpose at least some of them to hunt for adversaries in our DoD networks and even to perform full-spectrum operations. Although doing so will require a large investment of people, resources, and time, in the long run it will be cheaper to train Service personnel than to hire contractors. Moving to the JIE will make sharing and analytics easier while also boosting security. I know this sounds paradoxical but it is nonetheless true, as NSA has demonstrated in its Cloud capability. If we know what is happening on our networks, and who is working in them and what they are doing, then we can more quickly and efficiently see and stop unauthorized activities. We can also limit the harm from them and more rapidly remedy problems, whether in recovering from an incident or in preventing one in the first place. This is our ultimate objective for operations on our Department of Defense information architecture.

As we grow capacity, we are building cyber mission teams now , with the majority supporting the Combatant Commands and the remainder going to USCYBERCOM to support national missions. When we have built this high-quality, certified, and standardized force, we will be able to present cyber forces with known capability sets to our Combatant Commanders—forces they can train with, plan for, plan on, and employ like forces and units any other military domain. This gets at the essence of normalizing cyber capabilities for the Department of Defense. Furthermore, we want to increase the education of our future leaders by fully integrating cyber in our existing war college curricula. This will further the assimilation of cyber into the operational arena for every domain. Ultimately we could see a war college for cyber to further the professional military education of future leaders in this domain.

Conclusion

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to speak to you today. I hope you will agree with me that U.S. Cyber Command has made progress across the board in the last year, thanks to the support of Congress and our interagency and international partners, as well as the hard work of its many dedicated men and women. The novelist and

visionary William Gibson once noted “The future is already here, it’s just not evenly distributed.” We are seeing that future at U.S. Cyber Command. Cyber capabilities are already enhancing operations in all domains. We are working to contain the vulnerabilities inherent in any networked environment or activity while ensuring that the benefits that we gain and the effects we can create are significant, predictable, and decisive. If I could leave you with one thought about the course of events, it is that we have no choice but to normalize cyberspace operations within the US military and make them part of the capability set of our senior policymakers and commanders. I am ready to take your questions and to clarify our Command’s achievements and challenges, and to discuss any concerns that you might wish to share.