STATEMENT OF

GENERAL KEITH B. ALEXANDER

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS

AND CAPABILITIES

12 MARCH 2014

Chairman Thornberry, Ranking Member Langevin, and distinguished members of the Committee, thank you for the opportunity to speak to you today on behalf of the men and women of the United States Cyber Command (USCYBERCOM). As you know, this will be the last time I have the honor of talking about our Command's fine and dedicated Service members and civilian personnel before this Committee. It always gives me great pleasure to tell you about their accomplishments, and I am both grateful for and humbled by the opportunity I have been given to lead them in the groundbreaking work they have done in defense of our nation.

USCYBERCOM is a subunified command of U.S. Strategic Command in Omaha, Nebraska though based at Fort Meade, Maryland. It has approximately 1,100 people (military, civilians, and contractors) assigned with a Congressionally-appropriated budget for Fiscal Year 2014 of approximately $562 million in Operations and Maintenance (O&M), Research, Development, Test and Evaluation (RDT&E), and military construction (MILCON). USCYBERCOM also has key Service cyber components: Army Cyber Command/Second Army, Marine Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, and Air Forces Cyber/24th Air Force. Together they are responsible for directing the defense ensuring the operation of the Department of Defense's information networks, and helping to ensure freedom of action for the United States military and its allies—and, when directed, for defending the nation against attacks in cyberspace. On a daily basis, they are keeping U.S. military networks secure, supporting the protection of our nation's critical infrastructure from cyber attacks, assisting our combatant commanders, and working with other U.S. Government agencies tasked with defending our nation's interests in cyberspace.

USCYBERCOM resides with some key mission partners. Foremost is the National Security Agency and its affiliated Central Security Service (NSA/CSS). The President's recent decision to maintain the "dual-hat" arrangement under which the Commander of USCYBERCOM also serves as the Director of NSA/Chief, CSS means the co-location of USCYBERCOM and NSA/CSS will continue to benefit our nation. NSA/CSS has unparalleled capabilities for detecting threats in foreign cyberspace, attributing cyber actions and malware, and guarding national security information systems. At USCYBERCOM, we understand that re-creating a mirror capability for the military would not make operational or fiscal sense. The best, and only, way to meet our nation's needs today, to bring the military cyber force to life, and to exercise good stewardship of our nation's resources is to leverage the capabilities (both human and technological) that have been painstakingly built up at Fort Meade. Our nation has neither the resources nor the time to redevelop from scratch the capability that we gain now by working with our co-located NSA partners. Let me also

mention our other key mission partner and neighbor at Fort Meade, the Defense Information Systems Agency (DISA). DISA is vital to the communications and the efficiency of the entire Department, and its people operate in conjunction with us at USCYBERCOM on a constant basis. We all work in conjunction with the extensive efforts of several federal government mission partners, particularly the Department of Homeland Security (DHS), the Department of Justice and its Federal Bureau of Investigation (FBI), and other departments and agencies. We also work with private industry and allies in the overall mission of securing our networks, identifying threat actors and intentions, building resiliency for federal and critical infrastructure systems, and supporting law enforcement in investigating the theft and manipulation of data.

Allow me to review the highlights since our last posture hearing before the Committee a year ago. The main point I want to leave with you is that we in US Cyber Command, with the Services and other partners, are doing something that our military has never done before. We are putting in place foundational systems and processes for organizing, training, equipping, and operating our military cyber capabilities to meet cyber threats. USCYBERCOM and the Services are building a world class, professional, and highly capable force in readiness to conduct full spectrum cyberspace operations. Seventeen out of one hundred thirty-three projected teams have achieved full or "initial" operational capability, and those teams are already engaged in operations and accomplishing high-value missions. The Cyber Mission Force is no longer an idea on a set of briefing slides; its personnel are flesh-and-blood Soldiers, Marines, Sailors, Airmen, and Coast Guardsmen, arranged in military units that are on point in cyberspace right now. We are transforming potential capability into a reliable source of options for our decision makers to employ in defending our nation. Future progress in doing so, of course, will depend on our ability to field sufficient trained, certified, and ready forces with the right tools and networks to fulfill the growing cyber requirements of national leaders and joint military commanders. That is where we need your continued support.

The Threat Picture

The Department of Defense along with the Department of Homeland Security, the Department of Justice, and the Federal Bureau of Investigation have primary responsibilities to defend the United States in cyberspace and to operate in a global and rapidly evolving field. Our economy, society, government, and military all depend on assured security and reliability in this man-made space, not only for communications and data storage, but also for the vital synchronization of actions and functions that underpins our defenses and our very way of life. USCYBERCOM concentrates its efforts on defending

military networks and watching those actors who possess the capability to harm our nation's interests in cyberspace or who intend to prepare cyber means that could inflict harm on us in other ways.

Unfortunately, the roster of actors who concern us is long, as is the sophistication of the ways they can affect our operations and security. We have described some of these in previous hearings, and I know the Director of National Intelligence recently opened his annual World Wide Threat Assessment for Congress with several pages on cyber threats, so I'll be brief here.

I can summarize what is happening by saying that the level and variety of challenges to our nation's security in cyberspace differs somewhat from what we saw and expected when I arrived at Fort Meade in 2005. At that time many people, in my opinion, regarded cyber operations as the virtual equivalents of either nuclear exchanges or commando raids. What we did not wholly envision were the sort of cyber campaigns we have seen in recent years. Intruders today seek persistent presences on military, government, and private networks (for the purposes of exploitation and disruption). These intruders have to be located, blocked, and extracted over days, weeks, or even months. Our notion of cyber forces in 2005 did not expect this continuous, persistent engagement, and we have since learned the extent of the resources required to wage such campaigns, the planning and intelligence that are essential to their success, and the degree of collaboration and synchronization required across the government and with our allies and international partners. Through concerted efforts, and with a bit of luck, we are creating capabilities that are agile enough to adapt to these uses and others, and I am convinced we have found a force model that will give useful service as we continue to learn and improvise for years to come.

We have some key capability gaps in dealing with these increasingly capable threats. Cyberspace is a medium that seems more hospitable to attackers than defenders, and compared to what real and potential adversaries can do to harm us, our legacy information architecture and some of our weapons systems are not as "cyber robust" as they need to be. Our legacy forces lack the training and the readiness to confront advanced threats in cyberspace. Our commanders do not always know when they are accepting risk from cyber vulnerabilities, and cannot gain reliable situational awareness, neither globally nor in US military systems. In addition, the authorities for those commanders to act have been diffused across our military and the US government, and the operating concepts by which they could act are somewhat undefined and not wholly realistic. Further our communications systems are vulnerable to attacks. We need to rapidly pursue a defense in depth as we envision with the fielding of the Joint Information Environment.

These gaps have left us at risk across all the USCYBERCOM mission areas that I described above.

USCYBERCOM's Priorities

USCYBERCOM is addressing these gaps by building cyber capabilities to be employed by senior decisionmakers and Combatant Commanders. In accordance with the Department of Defense's *Strategy for Operating in Cyberspace*, the people of USCYBERCOM (with their NSA/CSS counterparts) are together assisting the Department in building:

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

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 a lack of momentum 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. USCYBERCOM, with its Service cyber components, NSA/CSS, and DISA, monitors the functioning of DoD networks, providing the situational awareness to enable dynamic defenses. Unfortunately, DoD's current architecture in its present state is not fully defensible. That is why the Department is building 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 IT efficiencies. The JIE, together with the cyber protection teams that I shall describe in a moment, will give our leaders the ability to truly defend our data and systems. Senior officers from USCYBERCOM and DISA serve on JIE councils and working groups, and together with leaders from the office of the DoD's Chief Information Officer, Joint Staff J6, and other agencies, are guiding the JIE's implementation (with NSA's support as Security Adviser). JIE has been one of my highest priorities as Commander, USCYBERCOM and Director, NSA/CSS.

***Trained and Ready Forces*:** Over the last year we have made great progress in building out our joint cyber force. When I spoke to you in March 2013 we had just begun to establish the Cyber Mission Forces in the Services to present to USCYBERCOM. This force has three main aspects: 1) Cyber National Mission Teams to help defend the nation against a strategic cyber

attack on our critical infrastructure and key resources; 2) Cyber Combat Mission Teams under the direction of the regional and functional Combatant Commanders to support their objectives; and 3) Cyber Protection Teams to help defend DoD information environment and our key military cyber terrain. On January 17, 2014 we officially activated the Cyber National Mission Force – the U.S. military's first joint tactical command with a dedicated mission focused on cyberspace operations. We have plans to create 133 cyber mission teams by the end of FY 2016, with the majority supporting the Combatant Commands and the remainder going to USCYBERCOM to support national missions. The teams will work together with regional and functional commanders according to a command and control construct that we are actively helping to forge and field.

The training for this force is happening now on two levels. At the team level, each cyber mission team must be trained to adhere to strict joint operating standards. This rigorous and deliberate training process is essential; it ensures the teams can be on-line without jeopardizing vital military, diplomatic, or intelligence interests. Such standards are also crucial to assuring intelligence oversight and to securing the trust of the American public that military operations in cyberspace do not infringe on the privacy and civil liberties of U.S. persons. Our training system is in the midst of certifying thousands of our people to high and joint military-wide standards.

At the individual level, we are using every element of capacity in our Service schools and in NSA to instruct members of the Cyber Mission Force teams. We have compiled a training and readiness manual, a "summer school" for cyber staff officers, and are shaping professional military education to enhance the cyber savvy of the force. To save time and space, furthermore, we have established equivalency standards to give individuals credit for training they have already taken in their Services and at NSA, with a board to adjudicate how much credit to confer for each course. Finally, we have established Job Qualification Records for team work roles to provide joint standards, further reinforcing common baselines of knowledge, skills and abilities across Service-component teams.

As our training system geared up to meet our need for trained operators and certified teams, sequestration-level reductions and furloughs last year seriously impeded our momentum. The uncertain budget situation complicated our training efforts; indeed, we had to send people home in the middle of our first-ever command and staff course last summer. Moreover, every day of training lost had cascading effects for the overall force development schedule, delaying classes, then courses, and then team certifications, to the point we are about six months behind where we had planned to be in training our teams. We are only now catching up to where we should have been months ago in building the Cyber Mission Force.

Increased Operational Awareness: Enhanced intelligence and situational awareness in our networks help us know what is happening in cyberspace. Our goal is to build a common operating picture, not only for the cyber activities of organizations based at Fort Meade but also across the U.S. government. We are moving toward this objective, for instance by coordinating the activities of the USCYBERCOM and NSA operations centers. Achieving it should let all who secure and defend our networks synchronize their activities, as well as see how adversarial and defensive actions can affect one another, which in turn enhances the efforts of planners and the predictability of the effects they seek to attain.

***Capacity to Take Action*:** The last year saw increased collaboration between defenders and operators across the US government and with private and international partners. USCYBERCOM played important roles in several areas. USCYBERCOM, for instance, has been integrated in the government-wide processes for National Event responses. This regularly exercised capability will help ensure that a cyber incident of national significance can elicit a fast and effective response at the right decisionmaking level, to include pre-designated authorities and self-defense actions where necessary and appropriate. In addition, USCYBERCOM participated in whole-of-government actions with partners like the Departments of State, Justice, and Homeland Security in working against nation-state sponsored cyber exploitation and distributed denial-of-service attacks against American companies. Finally, we already benefit from sharing information on cyber threats with the services and agencies of key partners and allies, and are hopeful that cybersecurity legislation will one day make it easier for the U.S. Government and the private sector to share threat data in line with what the Administration has previously requested.

***Operating Concepts*:** To oversee and direct the nation's cyber forces, as previously mentioned, we have established a National Mission Force Headquarters in USCYBERCOM at Fort Meade. This functions in parallel with analogous headquarters units (the four Joint Force Headquarters) for the Service cyber components, which themselves work with the NSA/CSS regional operating centers in Georgia, Texas, and Hawaii.

We can report some good news with respect to the realism of our cyber exercises, which put these operating concepts to the test. USCYBERCOM regularly participates in more than twenty Tier 1 Combatant Command, coalition, and inter-agency exercises. We also run a Cyber Wargame that looks five years into the future and includes industry and academic experts. USCYBERCOM's flagship exercises, CYBER FLAG and CYBER GUARD, are much more sophisticated now and are coupled directly with Joint Doctrine and the Force Model. CYBER FLAG, held each fall at Nellis Air Force Base in

Nevada, includes all the Service cyber components as well as inter-agency and international partners. CYBER FLAG 14 in November 2013 assembled more than 800 participants, included conventional maneuvers and kinetic fires in conjunction with cyber operations, and featured a much more realistic and aggressive adversary in its expanded virtual battlespace. In the past we were tentative about letting the cyber "red teams" loose, for fear they would impair expensive training opportunities for conventional arms. In our recent CYBER FLAG iteration last fall, we figuratively took the gloves off. Our defense consequently got its collective nose bloodied, but the defenders to their credit fought back and prevailed in chasing a determined foe out of our systems. For its part, CYBER GUARD is a whole-of-government event exercising state- and national-level responses to adversary actions against critical infrastructure in a virtual environment. It brings together DHS, FBI, USCYBERCOM, state government officials, Information Sharing and Analysis Centers, and private industry participants at the tactical level to promote shared awareness and coordination to mitigate and recover from an attack while assessing potential federal cyber responses. Finally, we are also building and deploying tools of direct use to "conventional" commanders in kinetic operations, some of which were most recently utilized in the latest Red Flag exercise run to keep our pilots at the highest degree of proficiency.

Where Are We Going?

Let me share with you my vision for what we at USCYBERCOM are building toward. We all know the US military is a force in transition. We are shifting away from legacy weapons, concepts, and missions, and seeking to focus—in a constrained resource environment—on being ready for challenges from old and new technologies, tensions, and adversaries. We have to fulfill traditional-style missions at the same time that we prepare for emerging ones, with new tools, doctrines, and expectations, both at home and abroad. We are grateful to Congress for lessening the threat of wholesale budget cuts called for by the Budget control Act. That makes it easier for the Department of Defense to maintain its determination to shield our cyberspace capabilities from the resource reductions falling on other areas of the total force. It is fair, and indeed essential, for you to ask how we are utilizing such resources while others are cutting back.

Our answer is that the trained and certified teams of our Cyber Mission Force are already improving our defenses and expanding the operational options for national decision makers, the Department's leadership, and joint force commanders. We are building this force and aligning the missions of the teams with intelligence capabilities and military requirements. Our cyber mission teams will bring even more capability to the "joint fight" and to whole-of-government and international efforts:

- USCYBERCOM is 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 USCYBERCOM in its national-level missions. In addition, we are integrating our efforts and plans with component command operational plans, and we want to ensure that this collaboration continues at all the Commands.

- Our new operating concept to enhance military cyber capabilities is helping to foster a whole-of-government approach to counter our nation's cyber adversaries. Indeed, USCYBERCOM planners, operators, and experts are prized for their ability to bring partners together to conceptualize and execute operations like those that had significant effects over the last year in deterring and denying our adversaries' cyber designs.

Here is my greatest concern as I work to prepare my successor and move toward retirement. Despite our progress at USCYBERCOM, I worry that we might not be ready in time. Threats to our nation in cyberspace are growing. We are working to ensure that we would see any preparations for a devastating cyber attack on our critical infrastructure or economic system, but we also know that warning is never assured and often not timely enough for effective preventive actions. Should an attack get through, or if a provocation were to escalate by accident into a major cyber incident, we at USCYBERCOM expect to be called upon to defend the nation. We plan and train for this every day. My Joint Operations Center team routinely conducts and practices its Emergency Action Procedures to defend the nation through inter-agency emergency cyber procedures. During these conferences, which we have exercised with the participation up to the level of the Deputy Secretary of Defense, we work with our interagency partners to determine if a Cyber Event, Threat or Attack has occurred or will occur through cyberspace against the United States. As Commander, USCYBERCOM, I make an assessment of the likelihood of an attack and recommendations to take, if applicable. We utilize this process in conjunction with the National Military Command Center (NMCC) to determine when and if the conference should transition to a National Event or Threat Conference.

We understand that security is one of the greatest protections for civil liberties, and that liberty can suffer when governments hastily adapt measures after attacks. At USCYBERCOM we do our work in full support and defense of the civil liberties and privacy of Americans. We do not see a tradeoff between security and liberty; we promote both simultaneously, because each enhances

the other. Personnel at USCYBERCOM take this responsibility very seriously. The tools, authorities, and culture of compliance at NSA/CSS give us the ability and the confidence to achieve operational success against some of the toughest national security targets while acting in a manner consistent with civil liberties and rights to privacy. That said, unless Congress moves to enact cybersecurity legislation to enable the private sector to share with the US Government the anomalous cyber threat activity detected on its networks on a real-time basis, we will remain handicapped in our ability to assist the private sector or defend the nation in the event of a real cyber attack. I urge you to consider the now daily reports of hostile cyber activity against our nation's networks and appreciate the very real threat they pose to our nation's economic and national security as well as our citizen's personal information. I am concerned that this appreciation has been lost over the last several months, as has the understanding that—when performed with appropriate safeguards—cyber threat information sharing actually enhances the privacy and civil liberties as well as the security of our citizens.

Conclusion

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to speak, and for all the help that you and this Committee have provided USCYBERCOM over the years. It has been my honor to work in partnership with you for these past 39+ years to build our nation's defenses. Never before has our nation assembled the talent, resources, and authorities that we have now started building into a cyber force. I am excited about the work we have done and the possibilities before us. This is changing our nation's capabilities, and making us stronger and better able to defend ourselves across the board, and not merely in cyberspace. We can all be proud of what our efforts have accomplished in building USCYBERCOM and positioning its men and women, and my successor, for continued progress and success.