STATEMENT OF

GENERAL KEITH B. ALEXANDER, USA

COMMANDER, UNITED STATES CYBER COMMAND

DIRECTOR, NATIONAL SECURITY AGENCY

CHIEF, CENTRAL SECURITY SERVICE

BEFORE THE

SENATE COMMITTEE ON APPROPRIATIONS

"CYBERSECURITY: PREPARING FOR AND RESPONDING

TO THE ENDURING THREAT"

12 JUNE 2013

Thank you very much, Chairwoman Mikulski and Ranking Member Shelby, for inviting me to speak to you and your colleagues. I am here representing the Department of Defense in general and the men and women, military and civilian, who serve at U.S. Cyber Command (USCYBERCOM) and the National Security Agency/Central Security Service (NSA/CSS). It is my honor to appear today with colleagues from the Department of Justice (DOJ) and its Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the National Institute of Science and Technology (NIST). I hope to describe some of the challenges we face in performing the difficult but vital missions of keeping U.S. national security systems secure, helping to protect our nation's critical infrastructure from national-level cyber attacks, and working with other U.S. Government agencies, state and local authorities, national allies, and the private sector in defending our nation's interests in cyberspace. Together we make up a team deeply committed to compliance with the law and the protection of privacy rights that works every day with other U.S. government agencies, industry, academia, citizens, and allies, for only our combined efforts will enable us to make progress in cybersecurity for the nation as a whole.

Defending the Nation in Cyberspace

I would like to start today by discussing the two elements of this team that I lead. USCYBERCOM is a sub-unified command of U.S. Strategic Command in Omaha, though we are based at Fort Meade. USCYBERCOM's mission is to plan, coordinate, integrate, synchronize and conduct activities to direct the operations and defense of Department of Defense

information networks. We also prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable traditional military activities, ensure U.S./Allied freedom of action in cyberspace, and deny our adversaries the ability to harm us or our allies. USCYBERCOM has three operational focus areas: defending the Nation, supporting the Combatant Commands, and defending DoD Information Networks. As I noted when I testified before the Armed Services Committee in March, USCYBERCOM will address these three operational focus areas with its new Cyber Mission Forces, organized into National Mission Teams, Combat Mission Teams and Cyber Protection Teams.

Due to the intersecting responsibilities of the two organizations, USCYBERCOM was placed at the headquarters of NSA/CSS at Fort Meade. NSA/CSS collects signals intelligence on our cyber adversaries; and provides information assurance strategies and technologies to protect our national security systems. The conduct of these two missions is critical to enabling cyber operations. NSA/CSS also has multiple, technical capabilities critical to the cyber mission area, such as high-performance computing and large-scale, distributed processing and data storage. These are just some of the components of what we call the cryptologic platform; it constitutes the collection of signals intelligence and communications security capabilities that since 1952 have served users ranging from national customers, to departmental analysts, to battlefield commanders. The defense of U.S. military networks depends on knowing what those who would harm us are doing in cyberspace, which in turn depends on intelligence produced by NSA and other members of the Intelligence Community regarding adversary intentions and capabilities.

Cyberspace is characterized by high levels of convergence of separate and different networks and technology that have come together to form something greater than the sum of the parts. In this regard, USCYBERCOM's co-location with NSA/CSS mirrors the convergence in cyberspace and is a direct result of that technological shift. What we have learned is that if convergence is the reality of the cyber environment, then integration must be the reality of our response. Co-location promotes intense and mutually beneficial collaboration in an operational environment in which USCYBERCOM's success relies on net-speed intelligence. Although they are separate and distinct organizations with their own missions and authorities, NSA/CSS is a major force multiplier for USCYBERCOM, pairing the Command's operators, planners, and analysts with the expertise and assistance of NSA/CSS' cryptographers, analysts, access developers, on-net operators, language analysts, and support personnel. These are close working relationships that enable seamless, deconflicted operations that are vital to the success of the cyber mission. Co-location also improves the deconfliction of operations; physical proximity enhances mutual understanding and awareness of mission areas and helps forge effective partnerships that serve both organizations and the nation well. Only a tightly integrated team, and tightly integrated solutions, can do what is required to address cyber threats at net speed.

I serve as the dual-hatted Commander, USCYBERCOM, and Director, NSA/Chief, CSS. The dual-hatting unifies the capabilities for full-spectrum cyber operations under a single official, maximizes the leverage of NSA/CSS cyber capabilities, capacities, and authorities, and establishes unity of effort in cyberspace for the Department of Defense. It allows deconfliction of the use of the cryptologic platform to occur with full knowledge of the needs of both organizations on a timely basis. Together, the people under my command and direction at

USCYBERCOM and NSA/CSS work in concert but always under their respective authorities. They direct the operation of the Department's information networks, detect threats in foreign cyberspace, attribute threats, secure national security information systems, and help ensure freedom of action for the United States military and its allies in cyberspace—and, when directed, defend the nation against a cyber attack.

In keeping with the DoD's *Strategy for Operating in Cyberspace*, USCYBERCOM and NSA/CSS 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) the capacity to take action when authorized. Indeed, with another key mission partner in DoD—the Defense Information Systems Agency (DISA), also based at Fort Meade—we are finding that our progress in each of these five areas benefits our efforts in the rest. We are improving our tactics, techniques, and procedures, as well as our policies and organizations. This means building cyber capabilities into doctrine, plans, and training – and building them in a way that senior leaders can plan and integrate such capabilities as they would capabilities in the air, land, and sea domains.

The imperative to accomplish this mission grows every day. We operate in a dynamic and contested domain that literally changes its characteristics each time someone powers on a networked device. Make no mistake: in light of the real and growing threats in cyberspace, our nation needs a strong DoD role in cyberspace. While we feel confident that most foreign leaders believe that a devastating attack on the critical infrastructure and population of the United States by cyber means would elicit a prompt and proportionate response, it is possible, however, that

some regime or cyber actor could misjudge the impact and the certainty of our resolve. In particular, we are not yet deterring the persistent cyber harassment of private and public sites, property, and data. Such attacks have not caused loss of life, but they have been destructive to both data and property in other countries. The remote assaults last summer on Saudi Aramco and RasGas, for example, rendered inoperable—and effectively destroyed the data on—more than 30,000 computers. Cyber programs and capabilities are growing, evolving, and spreading; 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 groups or even individuals who in their zeal to make some political statement do not know or do not care about the collateral damage they inflict on bystanders and critical infrastructure. The United States is already a target. Networks and websites owned by Americans and located here have endured intentional, state-sponsored attacks, and some have incurred degradation and disruption because they happened to be along the route to another state's overseas targets. Our critical infrastructure is thus doubly at risk. On a scale of one to ten, with ten being strongly defended, our critical infrastructure's preparedness to withstand a destructive cyber attack is about a three based on my experience. There are variations in preparedness across sectors, but all are susceptible to the vulnerabilities of the weakest.

Let me draw your attention to another serious threat to U.S. interests: the continuing and systematic cyber exploitation of American companies and enterprises, and the resulting theft of intellectual property. Many such incidents are perpetrated by organized cybercriminals, but foreign government-directed cyber operators, tools, and organizations are targeting the data of American and Western businesses, institutions, and citizens. Certain nations have a resourced

national strategy to grow their economies by intellectual property (IP) theft. They target any company with valuable IP or a leading position in its sector—and not just that company itself. Even companies that have protected their information have partners that could be "soft" targets. Are we susceptible? In the U.S., intrusions have occurred against the best in the security business. The collective damage that such intrusions inflict on 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 theft jeopardizes our economic well being.

The U.S. Federal Cybersecurity Team

No federal department or agency is solely responsible for addressing the cyber threat, and none has been designated as the federal cybersecurity lead because each brings unique authorities, resources, and capabilities to the effort. Cybersecurity requires a team approach, where the leadership and support roles change depending on the nature of the threat and the required response. Together, three departments carry out important roles and responsibilities as part of the broader U.S. federal cybersecurity team in order to provide for the nation's cybersecurity:

- The DOJ is the lead federal department responsible for the investigation, attribution, disruption and prosecution of cybersecurity incidents. Within the DOJ, the FBI conducts domestic collection, analysis, and dissemination of cyber threat intelligence.

- The DHS is the lead federal department responsible for national protection against, mitigation of, and recovery from domestic cybersecurity incidents. The DHS is also the lead for securing unclassified federal civilian government networks and working with owners and operators of critical infrastructure to secure their networks through risk assessment, mitigation incident-response capabilities.

- The DoD is ultimately responsible for defending the nation from attack in cyberspace, just as it is in all other domains. In the event of a foreign cyber attack on the United States with the potential for significant national security or economic consequences, the DoD, including USCYBERCOM with the support of NSA/CSS, will be prepared to respond.

These efforts depend on shared situational awareness and integrated operations across the U.S. government, state and local authorities, and international partners. Together, we are helping to increase our global situational awareness through our growing collaboration with federal government mission partners and other departments and agencies, as well as with private industry and with other countries. That collaboration allows us to better understand what is happening across the cyber domain, which enhances our situational awareness, not only for DoD but also across the U.S. government.

Under the joint leadership of DHS and NSA, the FBI and the other Federal Cybersecurity centers created a framework to describe cybersecurity functions and information exchanges and are now developing an implementation plan for an information sharing environment that will

create a cross-government shared situational awareness that is extensible to other partners such as the state and local governments and our allies. Implementing this capability to improve our collective response actions is one of the President's top cyber priorities for Fiscal Year 14.

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 today of the importance of this synergy across the Department, the government, and our public at large. Last fall the departments negotiated, and the President endorsed, a broad clarification of the responsibilities of the various organizations and capabilities operating in cyberspace, revising the procedures we employ for ensuring that, in the event of a cyber incident of national significance, we are prepared to act with all necessary speed in a coordinated and mutually-supporting manner. USCYBERCOM is also being integrated into the National Event response process, so that a cyber incident of national significance can elicit a fast and effective response, to include self-defense actions where approved, necessary, and appropriate.

As part of this progress, we in the federal government are working with state, local, international, and private partners. NSA/CSS, for example, is defining security dimensions that government and private users can utilize for "cloud" architectures, and has shown how we can manage large quantities of data and still preserve strong security. We have even shared the source code publicly so public and private architectures can benefit from it. USCYBERCOM has sponsored not only an expanding range of training courses but also two important exercises, CYBER FLAG and CYBER GUARD. The former is USCYBERCOM's major Command-level

exercise, the most recent iteration of which brought in international partners to practice force-on-force maneuvers in cyberspace. 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.

Resources

For the past five years, federal cyber-related spending and performance reporting have been organized around the Comprehensive National Cybersecurity Initiative (CNCI), from which NSA/CSS received a significant amount of funding to provide specialized capabilities and foundational support to address the cyber threat. Last summer – and planned as a yearly exercise - the Administration issued a data call, which includes CNCI and non-CNCI investments, in order to better understand and track cybersecurity and cyberspace operations funding. NSA/CSS's budget under this taxonomy represents spending under the major cybersecurity categories: (1) Prevent malicious cyber activity, (2) Detect, Analyze, and Mitigate Intrusions, and (3) Shape the Cybersecurity Environment. These investments are fundamental to our overall cybersecurity strategy to develop and deploy unique cyber capabilities that leverage the use of signals intelligence to enhance network defense. Additional investments in cyberspace operations provide the foundational infrastructure necessary to build those capabilities as well as support full spectrum cyberspace operations in direct support of Combatant Command

requirements (e.g., cryptanalysis, net-centric capabilities, data repositories, sensor deployments, and research).

From the operational perspective, the ultimate objective of cybersecurity is to deny the adversary any opportunity to exploit our systems. Doing so requires that we protect ourselves from both known and unknown threats as we execute our comprehensive strategy of hardening our networks, defending our networks, and leveraging all instruments of national power – both within our own networks and beyond. We have made significant progress in realizing the mission capabilities and cryptologic capacity required to meet the demands of operating in cyberspace. While there is still much work to do, I'd like to highlight a few of the ongoing efforts in implementing our strategy.

The Department of Defense is responsible for seven million networked devices and thousands of enclaves. USCYBERCOM and NSA/CSS work around the clock with DISA to monitor what is happening on global networks and the functioning of DoD's information enterprise. We are also helping the Department build 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 will be the base from which we can operate knowing that our networks are safer from adversaries. Senior officers from USCYBERCOM and NSA/CSS 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/CSS in particular serves as the Security Advisor to the JIE, and is defining the security dimension of that architecture.

Moving to the JIE will make sharing and analytics easier while also enhancing security. I know this sounds paradoxical but it is nonetheless true, as NSA/CSS has demonstrated in its cloud capability and its support for the Intelligence Community's growing Information Technology Enterprise (IC ITE). Let me emphasize our confidence that the JIE will save resources for the Department—moving to it will give us greater capability and security at less cost.

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. Last December, DoD 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 forces for STRATCOM in support of USCYBERCOM-delegated Unified Command Plan mission. 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 operating authorities under order from the Secretary of Defense and from my capacity as the Director of NSA/CSS. 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.

I must also mention our concerns over the ongoing budget uncertainty. Foremost in the minds of many of our people are the looming furloughs which entail up to 11 days without pay between 7 July and 21 September. While many of our personnel are exempted from the furloughs, others are not, and their absence will degrade our mission readiness and performance

this summer and beyond, and make the development of a strong and capable cyber force more problematic. Our people truly are our most important capability. We can and have showcased the incredibly valuable contributions made by our entire workforce daily in securing our networks, supporting our war fighters, and providing unique insights into foreign intelligence targets. I want to emphasize the harmful impact of furloughs on the vital mission and functions we perform and on the people we have entrusted to perform or enable them. Furloughs make hiring new personnel harder and will drive our best personnel away to jobs awaiting in the private sector. Our USCYBERCOM and NSA/CSS workforce, regardless of funding stream, is one that by definition seamlessly collaborates across the many functions and disciplines that constitute our capabilities and operations. All are essential to the whole.

Guarding Privacy and Civil Liberties

Let me emphasize that our nation's security in cyberspace is not a matter of resources alone. It is an enduring principle and an imperative. Everything depends on trust. We operate in a way that ensures we keep the trust of the American people because that trust is a sacred requirement. We do not see a tradeoff between security and liberty. It is not a choice, and we can and must do both simultaneously. The men and women of USCYBERCOM and NSA/CSS take this responsibility very seriously, as do I. Beyond my personal commitment to do this right, there are multiple oversight mechanisms in place. Given the nature of our work, of course, few outside of our Executive, Legislative and Judicial Branch oversight bodies can know the details of what we do or see that we operate every day under strict guidelines and accountability within one of the most rigorous oversight regimes in the U.S. Government. For those of you who do,

and who have the opportunity to meet with the men and women of USCYBERCOM and NSA/CSS, you have seen for yourself how seriously we take this responsibility and our commitment to earning and maintaining your trust.

Legislation

Although the February 2013 Executive Order will help raise the nation's cyber defenses, it does not eliminate the urgent need for legislation in these and other areas of cybersecurity. The Administration's legislative priorities for the 113th Congress build upon the President's 2011 Cybersecurity Legislative Proposal and take into account two years of public and congressional discourse about how best to improve the nation's cybersecurity. We support legislation that:

1. Facilitates cybersecurity information sharing between the government and the private sector as well as among private sector companies. We believe that such sharing can occur in ways that protect privacy and civil liberties, reinforce the appropriate roles of civilian and intelligence agencies, and include targeted liability protections;

2. Incentivizes the adoption of best practices and standards for critical infrastructure by complementing the process set forth under the Executive Order;

3. Gives law enforcement the tools to fight crime in the digital age;

4. Updates Federal agency network security laws, and codifies DHS' cybersecurity responsibilities; and

5. Creates a National Data Breach Reporting requirement.

In each of these legislative areas, we want to incorporate appropriate privacy and civil liberties safeguards.

The Administration wants to continue the dialogue with the Congress and stands ready to work with members of Congress to incorporate our core priorities to produce cybersecurity information-sharing legislation that addresses these critical issues.

Conclusion

Thank you again, Madame Chairwoman and Members of the Committee, for inviting me to speak to you today. I also thank you on behalf of the men and women of USCYBERCOM and NSA/CSS for your support, and for the support of Congress. We are working to mitigate 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 and to make them part of the capability set of our senior policymakers and commanders. We are working closely with our interagency partners as well as other DoD elements. This is a necessity, for, as I suggest above, our nation faces diverse and

persistent threats in cyberspace that cannot be defeated through the efforts of any single organization. Most cyber operations are interagency efforts, almost by definition. We have gained valuable insight from the great work of partners like the Departments of Justice, Commerce, and Homeland Security, as well as from the collaboration of industry, academia, and allies. Indeed, the flow of information and expertise across the commands, agencies, departments and foreign mission partners here and overseas is improving slowly but steadily. We have much to gain from this partnership, but perhaps not much more time left before our situation in cyberspace becomes even more worrisome than today. And now I look forward to your questions**.**