STATEMENT OF

GENERAL KEITH B. ALEXANDER

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

20 MARCH 2012

Thank you, Chairman Thornberry, and Ranking Member Langevin, for inviting me to talk to you about Cyber Command. I am here representing Cyber Command, with an authorized staff of 937, and operational Service cyber components totaling over 12,000 men and women, whose great work helps to keep our nation more secure. Their ranks include uniformed members of all the military Services and the Coast Guard, as well as civilians and officials from several federal agencies partnered with us in our missions. There is no finer group of Americans anywhere, and the work they do is vital to our security now and in the future. I am proud and humbled to be associated with them.

The Fiscal Year 2013 President's Budget for Cyber Command provides $182 million dollars and 937 personnel to perform our global mission. As demand to develop and integrate capabilities into cyber planning and operations continues to grow, we continue to work with the Department to shape our resource requirements and workforce to provide the necessary level of effort against growing mission sets and threats. I last spoke to the committee in open session just about a year ago. Since then, Cyber Command has made substantial progress in building capabilities to perform its missions. I hasten to add, however, that our nation's need for mission success has also grown, both in its scope and in its urgency. Secretary of Defense Panetta recently told Members that "our adversaries are going to come at us using 21st Century technology," including cyber threats. Chairman Dempsey amplified that statement, noting that we are "very concerned about cyber." Both emphasized that cyber is one of the areas slated for investment in an overall Defense budget that will be leaner in the future. The United States relies on access to cyberspace for its national and economic security. The task of assuring cyberspace access continued to draw the attention of our nation's most senior leaders over the last year, and their decisions have helped to clarify what we can and must do about developments that greatly concern us.

Cyber Command is, of course, a component of a larger, U.S. Government-wide effort to make cyberspace safer for all, to keep it a forum for vibrant citizen interaction, and to preserve our freedom to act in cyberspace in defense of our vital interests and those of our allies. Although Cyber Command is specifically charged (among other missions) with directing the security, operation, and defense of the Department of Defense's (DoD) information systems, our work and our actions are affected by threats well outside DoD networks; threats the nation cannot afford to ignore. What we see, both inside and outside DoD information systems, underscores the imperative to act now to defend America in cyberspace. In my time with you today, I want to talk about that larger, strategic context, to note some recent changes in the ways that we express our cyber posture in public, and to explain what these developments mean specifically for the progress of Cyber Command and the larger cyber enterprise.

Strategic Context

In framing my comments on our progress at Cyber Command, I have to begin by noting a worrisome fact: cyberspace is becoming more dangerous. The Intelligence Community's world-wide threat brief to Congress in January raised cyber threats to just behind terrorism and proliferation in its list of the biggest challenges facing our nation. You know this if you are a national leader or a legislator, a military commander, a corporate executive or chief information officer, or just an ordinary citizen shopping or spending leisure time on-line. Out of necessity, more and more of the time and resources that every American spends on-line are being consumed by tasks to secure data, encrypt drives, create (and remember) passwords and keys, and repeatedly check for vulnerabilities, updates, and patches. Americans have digitized and networked more of their businesses, activities, and their personal lives, and with good reason they worry more about their privacy and the integrity of their data. So has our military. Those Americans who are among the growing

number of victims of cybercrime or cyber espionage, moreover, are also spending their time trying to figure out what they have lost and how they were exploited.

Dangers are not something new in cyberspace, of course. Observers theorized about hypothetical cyber attacks on data and information systems twenty years ago. When I spoke to you last year, however, I noted the sort of threats that were once discussed in theoretical terms were becoming realities and actually being deployed in the arsenals of various actors in cyberspace. I specifically use the broader term "actors" instead of "states." In 2010 we saw cyber capabilities in use that could damage or disrupt digitally controlled systems and networked devices, and in some cases we are not sure whether these capabilities are under the control of a foreign government. Furthermore, we believe it is only a matter of time before someone employs capabilities that could cause significant disruption to civilian or government networks and to our critical infrastructure here in the United States.

We have long seen cyber capabilities directed by governments to disrupt the communications and activities of rival states, and today we are also seeing such capabilities employed by regimes against critics inside their own countries. Events during the Arab Spring last year offer a wealth of examples. As you know, popular protests against authoritarian rule raised hopes across the Maghreb and beyond—hopes that were organized, informed, and expressed in no small part by expanded capacity for communications and the new social media applications that use it. The response of the former regimes in Egypt, Libya, and Tunisia—and some current regimes as well—was to try to filter, disrupt, or even shutter these channels for news and communications, whether to stifle ongoing protests by their own citizens or to keep their peoples from hearing that discontent in other lands had toppled autocratic regimes. Some regimes, moreover, even reach out via cyberspace to harass political opponents beyond their borders.

Cyber crime is changing as well. In part this is due to heightened security and wariness among governments, businesses, internet service providers (ISPs), and average users. Law enforcement and ISPs, for example, have gotten better at identifying "botnets," banks of computers slaved together for criminal purposes, and have become more skilled at neutralizing them. But now the more sophisticated cyber criminals are shifting away from botnets and such "visible" means of making money and toward stealthier, targeted thefts of sensitive data they can sell. Some cyber actors are paying particular attention to the companies that make network security products. We saw digital certificate issuers in the U.S. and Europe hit last year, and a penetration of the internal network that stored the RSA's authentication certification led to at least one U.S. defense contractor being victimized by actors wielding counterfeit credentials. Incidents like these affect DoD networks directly, targeting them with similar malware, often spread by clever "phishing" e-mails that hit an information security system at its weakest point—the user. Nation-state actors in cyberspace are riding this tide of criminality. Some of these actors can and may turn their resources and power against U.S. and foreign businesses and enterprises, even those that manage critical infrastructure in this country and others. State-sponsored industrial espionage and theft of intellectual capital now occurs with stunning rapacity and brazenness, and some of that activity links back to foreign intelligence services. Companies and government agencies around the world are thus being looted of their intellectual property by national intelligence actors, and those victims understandably turn for help to their governments.

The expanding popularity of social media and wireless consumer electronics is driving cyber crime as well. More and more malware is written for wireless devices, particularly smartphones, and soon, we anticipate, for tablets as well. These criminal gangs are trying to exploit social media users and wireless networked systems, but can also exploit our Soldiers, Sailors, Airmen, and Marines in their purely social activities. Real and potential

adversaries can and do learn a great deal about our personnel, procedures, and deployments by monitoring the use that our people make of popular social media. As our military goes wireless these threats to our weapons systems, communications, databases, and personnel demand attention.

Finally, I need to mention a recent development of concern to us at Cyber Command and across our government and allies. Last year we saw new prominence for cyber activist groups, like Anonymous and Lulz Security that were encouraging hackers to work in unison to harass selected organizations and individuals. The effects that they intentionally and indirectly cause are chaotic and perhaps exaggerated in the popular media, but the work of preventing those effects from disrupting DoD information systems does draw attention and resources. We are also concerned that cyber actors with extreme and violent agendas, such as al Qaeda affiliates or supporters, could draw upon the experiences and ideas of more sophisticated hactivists and potentially use this knowledge for more disruptive or destructive purposes, though it remains unclear what the likelihood of such an event is.

Our National Cyber Posture

The American people have rightly come to expect broad and economical access to cyberspace. They have saved their personal information, business files, research projects, intellectual capital, and recreational pursuits in digital formats and stored in networked computing devices. Moreover, they have built social and professional webs of contacts in cyberspace—the all-important "who you know"—and have thus come to rely on the accessibility of these networks. Our military and our government have done likewise. This increased inter-connectedness of our information systems, combined with the growing sophistication of cyber criminals and foreign intelligence actors, has increased our risk. Our inter-connectedness is now a national security issue. Ensuring and securing our computing systems has focused the energies of

America's leadership at both ends of Pennsylvania Avenue and in the Cabinet departments. Recent decisions have helped to clarify our posture for defending net users and the nation in cyberspace, and have sent strong signals to anyone who might impair our interests in this domain.

The President confirmed our inherent right to protect ourselves against attacks in this domain, as in the traditional domains, last spring in his International Strategy for Cyberspace, saying "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country." We reserve the right to use all necessary means — diplomatic, informational, military, and economic — as appropriate and consistent with applicable international law. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible. As in the other domains, of course, the United States will seek to exhaust all options before employing military force, and will seek international support whenever possible. Cyber Command exists to ensure that the President can rely on the information systems of the Department of Defense and has military options available for his consideration when and if he needs to defend the nation in cyberspace.

President Obama and Secretary of Defense Panetta have recently reviewed our nation's strategic interests and issued guidance on our defense priorities. In Sustaining U.S. Global Leadership: Priorities for 21st Century Defense, the Secretary focused on protecting access throughout the domain. For Cyber Command, this means we must pay attention to the ways in which nations and non-state actors are developing asymmetric capabilities to conduct cyber espionage—and potentially cyber attacks as well—against the United States as well as our allies and partners. In this context, our cyber capabilities represent key components of deterrence. Since modern forces cannot operate

without reliable networks, we will invest in advanced capabilities to defend them even in contested environments.

The Department of Defense recently added detail to that position. In accordance with the President's International Strategy, the Department further explained our deterrent posture to Congress in its "Cyberspace Policy Report" last November. DoD's components, particularly Cyber Command, seek to maintain the President's freedom of action and work to dissuade others from attacking or planning to attack the United States in cyberspace. We will maintain the capability to conduct cyber operations to defend the United States, its allies, and its interests, consistent with the Law of Armed Conflict. Our indications and warning and forensic intelligence capabilities necessary to identify our enemies and attackers in cyberspace, moreover, are improving rapidly. As the Department's report to Congress noted, the co-location of Cyber Command with the National Security Agency provides our Command with "unique strengths and capabilities" for cyberspace operations planning and execution. I can assure you that, in appropriate circumstances and on order from the National Command Authority, we can back up the Department's assertion that any actor contemplating a crippling cyber attack against the United States would be taking a grave risk.

Cyber Command works with a range of partner agencies in the U.S. government and among our allies, along with parallel efforts in private industry, to strengthen the overall defense of our citizens, the nation, and allies in cyberspace. The Departments of Defense and Homeland Security collaborate on various initiatives, including the Defense Industrial Base (DIB) Cyber Pilot, a test program to establish a construct for Commercial Service Providers to provide managed security services enhanced by government threat information to Defense Industrial Base companies; and the Enduring Security Framework, an executive and working-level forum with key partners in the commercial technology marketplace.

Finally, I want to assure you that all of our work is performed with our responsibility to safeguard the privacy and civil liberties of U.S. persons very much in our minds. We take very seriously, in all of our operations, our duty to ensure that defending the Department of Defense's information systems and the nation's freedom to access cyberspace does not infringe on Americans' civil liberties, those rights guaranteed by the Constitution that I and every member of my Command swore an oath to uphold.

Building the Enterprise

Cyberspace has a scope and complexity that requires inter-agency, inter-service, and international cooperation. Within the Department of Defense, cyberspace issues are handled by our Command and a diverse set of other agencies and organizations, many of which have their own initiatives with government, allied, and industry partners. It is important to keep this context in mind as I review the efforts, accomplishments, and challenges of Cyber Command.

When I spoke to you a year ago, our Command had just become operational. Just a year later, we have a record of success. We are in action every day making the Department's networks more secure and its operations more effective. We are actively directing the operation of those networks and making commanders accountable for their security. Let me tell you about some of our recent successes:

- This time last year, sophisticated cyber intruders compromised the security of the algorithm employed in tokens distributed by the RSA Corporation. This was very serious news, since a large number of enterprises, including some in the Department of Defense, rely on

two-factor authentication using RSA tokens. Indeed, the systems of some non-DoD users were breached not long after the compromise by intruders exploiting the stolen certificates. Cyber Command had immediately recognized the danger to DoD information systems, warned those DoD networks at risk, and took swift mitigation efforts. We at Cyber Command directed and oversaw the replacement of all RSA tokens throughout DoD. Partly as a result of our actions, we have not seen any intrusions of DoD networks related to the RSA compromise.

- Just a few months ago, we saw an example of how Cyber Command has improved DoD's cybersecurity. In late 2010, cyber actors took advantage of a vulnerability in Adobe software that allowed them to install malicious software on computers whose users clicked on an apparently harmless link, a ruse called spearphishing. In that case, as Cyber Command was just beginning, several DoD networks/systems were breached and our experts could only react to stop files from being stolen and new breaches from being opened. A year later, by contrast, our defensive posture and cyber command and control processes had matured to the point where we were prepared not just to react but to counter such tactics. When another Adobe vulnerability was discovered in late 2011, Cyber Command quickly took action to ensure that no one would be able to use it against us. Sure enough, malicious cyber actors seized upon the vulnerability and used it to mount a spearphishing campaign targeting DoD networks. This time we were waiting and were able to block this campaign from exploiting our systems and acquiring any DoD files.

- The year 2011 might well be remembered as the Year of the Hacker. Various on-line groups garnered headlines for their efforts to publicize

causes of concern to them by breaching the security of government and private networks. The on-line collective calling itself Anonymous, to mention just one of these groups, announced several attempted attacks against Department of Defense information systems. Cyber Command was able to direct and integrate pro-active defensive cyber operations to successfully counter these threats. Over the past year, there have also been related, well-publicized examples of major exploitations or attacks against Defense contractors and other holders of intellectual property vital to our national security. The Cyber Command-led defense of the Department's information systems, however, prevented any of these threat actors from having a similar effect against DoD networks. Finally, the investigation of the WikiLeaks breach continued, and its progress was closely followed by the hacker groups. In response to the WikiLeaks breach, Cyber Command was able to direct actions across the Department that quickly reduced risks to DoD information. These measures supported operational Commanders exercising their accountability for cybersecurity in their units.

I'd be pleased to give you more details on these events in closed session, and to tell you about still others that remain too sensitive to mention here.

I am proud of this record of success but aware that more needs to be done by Cyber Command as part of the larger cyber enterprise that includes the National Security Agency/Central Security Service (NSA/CSS), the Service cyber components, and the Defense Information Systems Agency (DISA). I foresee five challenges over the coming year that Cyber Command will face and continue to address. Those areas are the following:

1] Concept for Operating in Cyberspace: Every domain, by definition, has unique features that compel military operations in it to conform to its physical

or relational demands. Doctrine, tactics, techniques, and procedures have been under development for millennia in the land and maritime domains, for a century in the air domain, and for decades in space. In the cyber domain, however, we are just beginning to craft new doctrine and tactics, techniques, and procedures. At the strategic level, we are building our organizational structures to ensure we can deliver integrated cyber effects to support national and Combatant Commander requirements; we are developing doctrine for a pro-active, agile cyber force that can "maneuver" in cyberspace at the speed of the internet; and we are looking at the ways in which adversaries might seek to exploit our weaknesses. At the operational level, our objectives are to establish a single, integrated process to align Combatant Commanders' requirements with cyber capabilities; to develop functional emphases in the Service cyber components; and to draft a field manual or joint publication on cyber operations and demonstrate proof of concept for it. Finally, rapid deconfliction of operations is required, and that is garnering leadership attention as well. We are currently working closely with two of the geographic combatant commanders. Our goal is to ensure that a commander with a mission to execute has a full suite of cyber-assisted options from which to choose, and that he can understand what effects they will produce for him. Though we can only work such an intensive process with two of the combatant commanders at this time, we will be able to reach out eventually to all of the combatant commands.

2] Cybersecurity Responsibilities: Defending the nation in cyberspace requires a coordinated response among several key players from throughout the government. It takes a cross-government team to mature and implement an effective cyber strategy for the nation. From my perspective, there are three key players that make up this team:

- Department of Homeland Security – lead for coordinating the overall national effort to enhance the cybersecurity of U.S. critical infrastructure, and ensuring protection of the civilian federal government (.gov) networks and systems.
- Federal Bureau of Investigation (FBI) – responsible for detection, investigation, prevention, and response within the domestic arena under their authorities for law enforcement, domestic intelligence, counterintelligence, and counterterrorism. Importantly, when malicious cyber activity is detected in domestic space, the FBI takes the lead to prevent, investigate, and mitigate it.
- Department of Defense / Intelligence Community / NSA / Cyber Command – responsible for detection, prevention, and defense in foreign space, foreign cyber threat intelligence and attribution, security of national security and military systems; and, in extremis, defense of the homeland if the Nation comes under cyber attack from a full scope actor.

Cyber Command is working to ensure we have identified the roles and responsibilities correctly to accomplish our mission. Overall, our most pressing need across the government is to ensure we can see threats within our networks and thus address malware before it threatens us. Foundational to this is the information sharing that must go on between the federal government and the private sector, and within the private sector, while ensuring appropriate measures and oversight to protect privacy and preserve civil liberties. We welcome and support new statutory authorities for DHS that would ensure this information sharing takes place; an important reason why cyber legislation that promotes this sharing is so important to the nation. Finally, we are working within the Department and Administration on establishing the Rules of Engagement and criteria upon which Cyber Command will act. We are working with the Joint Staff to develop a decision

framework that allows us to identify threats and ensure senior leaders can share information rapidly and take action, if necessary.

3] Trained and Ready Force: At present we are critically short of the skills and the skilled people we as a Command and a nation require to manage our networks and protect U.S. interests in cyberspace. Our prosperity and our security now depend on a very skilled technical workforce, which is in high demand both in government and industry. We in DoD need to build a cyber workforce that can take action quickly across the full range of our mission sets as necessary. This will require us to adopt a single standard across the Department and the Services, so that we can truly operate as a single, joint force. In order to achieve our goals in this area by 2014, we must build a skilled force capable of full-spectrum cyber operations across a continuum of threats. We also need to build our workforce at Cyber Command and the Service Cyber Components so that, in extremis, we have the capability to defend the nation in cyberspace. We are reviewing recruitment and incentive programs in order to build and retain the best of the best cyber defenders, and we are working to standardize, track, and manage the training needed for all cyber personnel.

Let me mention one of the ways in which we are building the cyber force. Last fall we sponsored our first major tactical exercise, which we called CYBER FLAG (after the RED FLAG exercise that has trained generations of fighter pilots since the 1970s). This was a large, multi-day affair, in which operators from our Service cyber components engaged in realistic and intense simulated cyber combat against "live" opposition. This unprecedented exercise attracted a great deal of interest from senior leaders in the Pentagon and other departments and agencies, and dozens of observers attended its sessions. Nevertheless, CYBER FLAG was no mere drill, but a training exercise for those necessarily engaged in cyber operations now. The lessons that network

operators learned first-hand in CYBER FLAG are being applied daily in defense of our networks and in support of national policy goals.

4] Defensible Architecture: Our current information systems architecture in the Department of Defense was not built with security uppermost in mind, let alone with the idea of operationalizing it to enable military missions. Instead, we have seven million networked devices in 15,000 DoD network enclaves. Our vision is to fashion that architecture into an operational platform, not just a channel for communications and a place for data storage. To do so, our DoD cyber enterprise, with the Department's Chief Information Officers, DISA, and Cyber Command helping to lead the way, will build a common cloud infrastructure across the Department and the Services that will not only be more secure but more efficient—and ultimately less costly in this time of diminishing resources—than what we have today.

Cyber Command will directly benefit from this in its mission of directing the security, operation, and defense of DoD information systems. Our strategic objective is to reduce the attack surface of our critical networks that is available to adversaries, enabling us to "Defend and Jump" as needed. Our operational objectives are to reduce the number of network enclaves to the minimum possible; to implement a common cloud-based infrastructure to improve security across all of DoD; to move to a more secure model for data and services with better tagging and metadata; to implement identity-based access controls to services, as well as attribute-based access controls to control who can use those data; and finally to grow the capability to rapidly reconfigure the single network in response to mission requirements or enemy actions.

The NSA has begun making this vision a reality, with collateral benefits for Cyber Command in the process. The agency has sharply consolidated the number of desktop applications, closed half its help desks, trimmed the

number of data centers required, and saved money through corporate management of software licenses. Similar actions taken Department-wide will not only improve the security of the DoD's networks but also reduce its information technology costs, freeing money for other purposes and allowing for a re-dedication of cyber personnel to more urgent needs.

5] Global Visibility Enabling Action: We cannot wait for the implementation of that vision of a defensible architecture, however, to improve our situational awareness. Our commanders and our Services need to know what's happening inside and outside our networks, but at present we cannot even develop a definitive picture of the 15,000 DoD network enclaves and lack the capability to easily understand what is happening as it occurs. Furthermore, we must know in real time when and how the internet and the overall cyber environment inside and outside the United States are threatened in order to counter those threats. In this area, our strategic objectives are to enable unity of effort across DoD, the federal government, private partners and allied nations; to develop faster, more comprehensive, and timelier warning of threats against DoD networks and critical infrastructure; and to move beyond situational awareness to enabling integrated operational responses in cyberspace. Our operational objectives are to gain visibility of, and fuse information from, our own and public networks to enable action; to partner with the interagency, private infrastructure providers and global partners to share information; and to build capabilities to empower decision makers.

Cyber Command Major Accomplishments (March 2011 to March 2012)

<u>Operational Impacts</u>

Common Operating Picture (COP) Exercise: Cyber Command Joint Operations Center, the NSA/CSS Threat Operations Center and the DoD Cyber Crime Center participated in a White House-led National Level Exercise to test the

federal government's ability to develop a COP appropriate for White House-level consumers.

Cyber Training Advisory Council (CYTAC) Creation: The CYTAC is an advisory and coordination committee established to improve the quality, efficiency, and sufficiency of training for computer network defense, attack, and exploitation that will work to coordinate and standardize cyber training across all military services, Cyber Command, and NSA.

National Reconnaissance Office (NRO) War Game THOR'S HAMMER: Cyber Command personnel supported NRO's space and cyber wargame that increased the participant's understanding of critical space asset capabilities and their vulnerabilities to cyber attacks. Additionally, the wargame highlighted the interrelationship between space security and cyberspace security.

DHS National Cyber Incident Response Program: Synchronized DHS National Cyber Incident Response Program (NCIRP) with the DoD's Cyberspace Conditions alert system to facilitate future actions.

Global Cyber Synchronization Conference: Hosted the second Global Cyber Synchronization Conference on behalf of USSTRATCOM to integrate operational planning requirements across the combatant commands.

Policy and Doctrine

The Administration is working with the Congress to finalize cybersecurity legislation. Within the Administration, there is a strong and unified working relationship between DoD, DHS and NSA on cybersecurity matters; and NSA, NIST and DHS are closely partnered to address cybersecurity standards.

Senate Cybersecurity Exercise: Members of the Senate participated in a cybersecurity exercise on 7 March 2012 as the result of an all-Senate cybersecurity threat briefing given by the White House and Departmental Secretaries on 1 February 2012.

Support to Operations

Cyber Command Cyber Support Element (CSE) Placements: Working with the combatant commands to place a CSE at each COCOM tailored to their mission support requirements for cyberspace operations. Cyber Command has a full CSE deployed to USCENTCOM, a partial CSE to PACOM, and expects to deploy a CSE to USAFRICOM and USSOCOM within 6 months.

Cyber Command Force Management Workshop: The Cyber Command Force Management Workshop held in November brought together service cyber components to discuss Cyber Command support for the Combatant Commanders.

Trained and Ready Cyber Forces: Cyber Command, NSA and the military's cyber service components completed development of the Joint Cyberspace Training and Certification Standards (JCT&CS) document that will serve as the common foundation for training all cyber operators to unified standards across the DoD.

Enhancing Defenses

GLOBAL THUNDER 12: The Cyber Command Joint Operations Center (JOC) supported USSTRATCOM's annual Field Training Exercise (FTX) designed to validate our Nuclear Command Control Communications (NC3) OPLAN tasks. The JOC supported this FTX with reporting, analysis, conducting de-confliction, and responding to cyber related events.

Cyber Command Support to NIMBLE GHOST: Cyber Command worked with the Joint Staff for this DoD exercise to provide a forum for senior DoD leaders to examine policies and procedures that enable the defense of DoD critical U.S. networks and explore the department's ability to respond to a major cyberspace attack.

Building Team Cyber

DHS Blueprint for a Secure Cyber Future: Offered substantive comments in response to a review of DHS' draft Blueprint for a Secure Cyber Future; the Cybersecurity Strategy for the Homeland Security Enterprise.

Enhanced DHS and DoD Cybersecurity Operational Collaboration: Efforts remain underway by DHS and DoD to clarify responsibilities, assign specific actions, and establish timelines for implementing the DHS-DoD Joint Cybersecurity Vision in a cybersecurity work plan.

Tri-Lateral Defense Cyber Contact Group: Cyber Command and NSA personnel attended the Tri-Lateral Defense Cyber Contact Group (DCCG) completing a planning-focused tabletop exercise with the United Kingdom, Australia, USSTRATCOM, and OSD(P); used to develop a listing of issues that impede our ability to conduct cyberspace operations trilaterally.

Conclusion

We are working on all five of these focus areas simultaneously because they all demand our attention and because progress in each depends on progress in the others. Our capabilities across the board have to improve together, or good ideas in one area can be undermined by continuing weakness in another. We are moving with all deliberate speed, moreover, because the

American people will rightfully want results, not excuses, as we defend our nation.

In conclusion, allow me to thank you again for inviting me here to talk about the achievements and the plans of Cyber Command. Cyberspace provides both incredible opportunities and significant challenges for the Department of Defense and the nation. Cyber Command is part of a whole-of-government effort to capitalize on those opportunities, and to reduce and mitigate the uncertainties. With your continued support, I have no doubt that the hardworking and capable men and women of the Command will rise to those challenges and continue to make our nation proud of their accomplishments. And now I look forward to continuing this dialogue with you, both here and in the months ahead.