STATEMENT OF

DR. JAMES N. MILLER
PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE
FOR POLICY

BEFORE THE

HOUSE OF REPRESENTATIVES
COMMITTEE ON ARMED SERVICES
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

MARCH 16, 2011

Chairman Thornberry, Ranking Member Langevin, and members of the subcommittee, thank you for inviting me to discuss Department of Defense (DoD) efforts in cyberspace, and the role of U.S. Cyber Command (USCYBERCOM). I am very pleased to join the USCYBERCOM Commander and National Security Agency (NSA) Director, General Keith Alexander.

The Department is investing heavily in information technology – $38.4 billion proposed for FY2012 – because it is an enormous force multiplier for military, intelligence, and business operations. In fact, DoD has over 15,000 networks and seven million computing devices, across hundreds of installations in dozens of countries around the globe.

Yet DoD's networks – as massive as they are – represent only part of our nation's growing reliance on cyberspace. Virtually every realm of civilian life now depends upon access to the Internet and other data-transmission networks. We use these networks every time we draw money from an ATM, open a webpage, or use our cell phones. With this reliance comes vulnerability; now that so many of our essential civilian and military functions depend on computer networks, we must recognize that any large-scale interference with such networks represents a potentially significant threat to our national security.

Understood in this context, DoD's proposal to spend $3.2 billion for cybersecurity in FY2012, including $159.7 million for USCYBERCOM, represents a sound investment in our national security.

We recognize that in the current fiscal climate, we must make hard choices about how we allocate scarce resources – both within the Pentagon and across the government. That is why I want to briefly describe the threats and vulnerabilities we face in cyberspace – as well as our plans to address them.

Threats and Vulnerabilities

DoD networks are attacked thousands of times each day, and scanned for vulnerabilities millions of times each day. Over one hundred foreign intelligence agencies are attempting to get into DoD's networks. Unfortunately, some incursions – by both state and non-state entities – have succeeded. These breaches have occurred mostly on unclassified networks, but in some cases on our classified networks as well.

The capabilities of state and non-state actors to exploit, disrupt, or even destroy DoD information systems are increasing. State actors are boosting their investments in cyberspace capabilities, and pose a considerable threat to U.S. cybersecurity. Al-Qaida, the Taliban and Hizbollah have long used cyberspace to plan their operations and influence global populations. Al-Qaida has vowed to launch a cyber attack on the United States. As technologies improve, non-state adversaries will be capable of conducting increasingly sophisticated cyberspace operations.

The theft of valuable information is to date the most concerning consequence of cyber intrusions. Over the last several years, malicious actors have stolen terabytes of data – including information used in the development of weapons systems – from companies in the U.S. defense industrial base (DIB). Leading information technology companies have also lost intellectual property as a result of sophisticated operations perpetrated against corporate infrastructures. More recently, critical infrastructure has been targeted, including our electric grid and the financial-services sector.

Moreover, cyber threats do not come exclusively from the outside. To the extent that we succeed in improving our defenses against external actors – and we must do so – outside actors will have greater incentives to try to use insiders to gain access to our networks. As we have

witnessed in WikiLeaks, insiders may sometimes prove willing to help disseminate sensitive information, even if it puts at risk the lives of many who support the United States, and damages U.S. national security.

One of the complexities of cybersecurity is that the distinction between "external" and "internal" threats can be blurred. That's because some of the gravest threats can be located in the networks themselves, and in the worldwide chain of suppliers we rely on to build our cyberspace infrastructure in the first place.

The global distribution of information-technology (IT) manufacturing means that software and hardware are at risk of being tampered with before they are linked together in an operational system. Tampering can even occur as part of regular maintenance and updating functions that modern IT equipment requires. Counterfeit hardware and software have been found in DoD systems already. We must remain alert to the possibility that "rogue code," "backdoors," and "kill switches" could be written into computer chips used by the Department or by other U.S. critical infrastructure.

In the face of this urgent threat, the Department of Defense is undertaking five initiatives to reduce its vulnerability. Because cybersecurity is a "team sport," two of our five strategic initiatives focus on partnerships with other government agencies, private companies, and allied nations.

1. Treating Cyberspace as a Domain for Organizing, Training, Equipping, and, When Directed, Operating

For the purposes of organizing, training, equipping, and, when directed, operating our forces, DoD recognizes cyberspace as a domain for military activities, analogous to the maritime,

air, land, and space domains. This understanding is essential for allowing DoD to clearly establish and achieve its cyberspace missions.

This initiative is not about "militarizing" cyberspace, any more than maintaining the U.S. Navy is about "militarizing" the ocean. Rather, our posture acknowledges a basic reality: Cyberspace presents security challenges that are too novel and too serious for it to be treated as an add-on to our traditional operations on land, at sea, or in the air. Just as in other domains, the Law of Armed Conflict applies to our activities in cyberspace, and civil liberties and privacy rights must be protected.

In order to focus DoD's cyberspace efforts, the Department established USCYBERCOM, as a subordinate command to United States Strategic Command. USCYBERCOM reached initial operating capability on May 21, 2010, and final operating capability on October 31, 2010.

DoD has requested $159 million for USCYBERCOM in FY2012. This includes:

- Facilities at Fort Meade, Maryland ($18M);
- Personnel, including 330 U.S. Air Force civilian billets ($47M);
- Information Technology and Communications support, including information technology fee-for-service, hardware, and software, as well as multiple networks and enclaves ($17M);
- Operations for day-to-day supplies, travel, training and support for the design of a Joint Operations Center ($36M);
- Research, development, test and evaluation ($26.0M), including a joint threat incident database and an Internet Service Provider Test Bed to create realistic environments; and
- Military construction ($15.0M).

Each of the military Services has established component commands of USCYBERCOM to effectively organize, train and equip America's soldiers, sailors, airmen and Marines for cyberspace operations. All four Services are developing service-specific capabilities, requirements, and skills for future cyber operations. In addition to taking steps to ensure that our DoD-operated networks, systems, and net-centric warfighting capabilities are available, all combatant commands and the Services must also prepare to operate in a "degraded cyber environment" in which cyberspace access is not assured or could be interrupted. To better understand this rapidly unfolding area, DoD conducts red-team assessments about future cyber threats to inform its strategic and operational planning.

All of these measures help ensure the U.S. military is prepared, if directed, to conduct full-spectrum cyberspace operations. Whether protecting U.S. interests in cyberspace or supporting broader military operations, our force needs to be as prepared to operate in cyberspace as it is in the traditional land, air, sea, and space domains.

2. Employing New Operational Concepts

DoD's second strategic initiative is to employ new defense operating concepts to protect our networks and systems. This includes advanced tools for cyberspace hygiene and active cyber defenses.

The first layer of defense is enhanced cyber hygiene, which includes such seemingly mundane but essential measures as updating the virus definitions of protective software. In addition to systems that ensure each DoD computer has "downloaded the patch," we now have host-based security services that can better map our systems, determine who is using them, and detect suspicious behavior.

Active cyber defense is crucial to detecting and stopping threats to our systems. It includes a perimeter defense of the dot.mil domain that screens incoming traffic for malicious code and malware. Because no perimeter defense is fail-proof, DoD also hunts on its own networks – looking for anomalies like viruses, worms and other software that could cause damage to our networks and systems. The Department has requested increased funds to carry out this protective self-surveillance, and to stop the intrusions that are found.

In addition to these measures, DoD is conducting research and development of new defense operating concepts, including the use of multiple networks to add resiliency; new "clean-slate" architectures to secure networks against the insider threat; and the use of cloud computing, virtualization, and advanced encryption.

3. Working with Other Government Agencies and the Private Sector

DoD's third strategic initiative is to work closely with other U.S. government departments and the private sector to create a national approach to cybersecurity. To this end, DoD supports the efforts of DHS, the lead department for protecting the Nation's critical networks.

To allow the Department of Homeland Security (DHS) to draw upon the cybersecurity capabilities already established by the National Security Agency and USCYBERCOM, Secretary of Defense Gates and Secretary of Homeland Security Napolitano signed a Memorandum of Agreement (MOA) on September 27, 2010. This agreement establishes a Joint Coordination Element at NSA, led by a senior DHS official with an NSA Deputy, which will improve the synchronization of our operational planning, help develop threat assessments, provide intelligence support, and allow for the joint development of new capabilities. A dedicated civil-liberties and privacy office supports this effort.

DoD works with other departments and agencies as well, as demonstrated by the Defense Cyber Crime Center's partnership with the FBI and other law enforcement agencies to create the National Cyber Investigative Joint Task Force (NCIJTF).

A great deal of sensitive but unclassified information resides on the networks of companies that work with our military, including approximately 2,600 cleared defense contractors. In 2007, DoD initiated a pilot program to determine whether the Department could help improve the cybersecurity of these affiliated systems. This three-year pilot program, with 36 different companies, significantly increased information sharing about the threats faced by companies, as well as information about how best to defeat those threats. Accordingly, DoD is requesting $113 million over the Future Years Defense Program (FYDP) to upgrade this pilot to a full program. We are also exploring other pilot projects with industry that would allow DoD to further extend its suite of cybersecurity capabilities to companies in the defense industrial base.

Pilot programs figure into the Department's strategy to protect or supply chain as well. The pilots that we have developed, if successful, will move towards full operational capability by FY2016, and will help DoD to reduce risks in the components that make up our operational systems.

4. Build Relationships with Allies and Partners

DoD's fourth strategic cyberspace initiative is to build robust relationships with U.S. allies and international partners. The Internet is a network of networks comprised of thousands of Internet service providers (ISPs) and billions of end users across the globe. No single state or agency can maintain effective cyber defenses on its own. DoD, in coordination with the State Department and other agencies of the U.S. government, will seek strong international relationships to defend U.S. and allied interests in cyberspace. The development of shared

situational awareness and warning capabilities will increase collective cybersecurity. Crucially, these partnerships will help us develop a global cyber-forensics capability to identify and track those responsible for incursions as well. In this new era, any hope that we have of deterring potential adversaries depends on our establishing accountability, and this will require extensive international cooperation.

To deter malicious behavior in cyberspace, DoD also supports the effort to define and promote international norms and principles regarding cyberspace. By clarifying acceptable behavior, enabling international communication, and minimizing the potential for misunderstanding and escalation, such standards will provide a foundation for the deterrence of malicious activities.

DoD has worked closely to build collective cyber defenses with Australia, Canada, New Zealand, and the United Kingdom. Over the last year, DoD has expanded its collaboration to include NATO. The Deputy Secretary of Defense travelled to Brussels twice over the last year to clarify the importance of cyberspace in NATO's new strategic concept and to help define an alliance agenda for rapidly deploying more advanced cyber defenses. DoD has initiated discussions with other allies and partners as well; working closely with the State Department, DoD will continue to explore new opportunities for international cooperation in cyberspace.

5. Workforce Development and Technological Innovation

The last initiative that I want to discuss – but far from the least important – is our effort to build a pool of talented civilian and military personnel to help DoD achieve its cyberspace missions, and to accelerate technological innovation.

Within DoD and across the government, the development of a cybersecurity workforce is a matter of national security. To build a capable cyber workforce, DoD will focus on attracting

talented personnel in the early stages of their careers. DoD will expand its educational scholarships, like the Information Assurance Scholarship Program, the Scholarship for Service program, and the U.S. Cyber Challenge. The Cyber Patriot program, one of the world's largest high-school cyber defense competitions, will help DoD to develop a talent base for future defense and national-security missions. Going forward, DoD will seek to enhance the Information Technology Exchange Program. This program, which is just getting underway, will allow for the expanded exchange of IT and cybersecurity personnel between government and industry.

DoD is fortunate to have access to a great deal of relevant expertise already – our National Guard and Reserve personnel include many advanced technology professionals who have a strong academic or professional grounding in cyber-related issues. It is incumbent upon the Department to utilize this current and future expertise as much as possible – breaking down traditional organizational barriers wherever they impede our efforts to put the best men and women on the front lines of our nation's cyber defense.

Our organizational challenges in cyberspace are not limited to the assignment of our personnel. They also haunt our acquisition systems – with potentially harmful results for our national security. It currently takes the Department of Defense approximately 81 months to make new computing systems operational. This means that by the time DoD has fielded its computing systems, they are already three to four generations behind the state of the art.

We must adjust DoD's acquisition processes to reflect the life cycle of technology development and the different uses to which IT is put. This means operating at cycles of 12 to 36 months as opposed to seven or eight years. DoD also needs to test and develop its systems on an incremental basis, rather than through the simultaneous deployment of large, complex

systems, that has proved so problematic. Through its legislation on IT acquisition reform, Congress has given the Department the tools to do better, and we must do so.

Our current procedures compel us to make long-term predictions about the future state of network technology – and then lock ourselves into the products and programs that emerge from those prognostications. In a field as dynamic and fluid as cyberspace, this is a recipe for high-stakes failure. We need a much more responsive approach, one that will allow for modular, adaptive investments and technological enhancements.

Even as DoD works to accelerate the deployment of new technologies, we must enhance security measures in procuring software and hardware. No backdoor can be left open; no system installed without proper vetting. To this end, DoD has recently announced several important initiatives to strengthen DoD's cyberspace technological capabilities.

- DoD is requesting $500 million in new Defense Advanced Research Projects Agency funds over the FY2012-2016 FYDP for cyberspace technologies, with a focus on areas like cloud computing, virtualization, and encrypted processing.
- The Department will continue to execute our cybersecurity pilot programs, as funded in FY2010, which provide seed capital to leading-edge technology companies to develop dual-use technologies that serve America's cybersecurity needs.
- We are developing a National Cyber Range that will help DoD and the U.S. government to operate successfully in a contested cyber environment. This facility will create models of the Internet and various networks, affording the military, other U.S. government agencies, the private sector, and potentially international allies and partners the opportunity to test new concepts and simulations at an effective scale. DoD is working

with other agencies of the U.S. government to create a transition plan now and to manage the issues associated with the conversion.

Conclusion

Thank you for this opportunity to describe some of the challenges the Department of Defense faces in cyberspace. With help from Congress, DoD is moving aggressively to protect our networks and help ensure our nation as a whole is better able to defend itself against threats in cyberspace. We have made significant strides in the last year – and I believe that our agenda is robust. I look forward to working with Congress to ensure we have the necessary capabilities to keep our country safe and our forces strong. I look forward to your questions.