STATEMENT OF

MR. THOMAS ATKIN

ACTING ASSISTANT SECRETARY OF DEFENSE FOR

HOMELAND DEFENSE AND GLOBAL SECURITY

OFFICE OF THE SECRETARY OF DEFENSE;

LIEUTENANT GENERAL JAMES K. MCLAUGHLIN

DEPUTY COMMANDER, U.S. CYBER COMMAND;

AND BRIGADIER GENERAL CHARLES L. MOORE JR.

DEPUTY DIRECTOR GLOBAL OPERATIONS (J-39), JOINT STAFF

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

22 JUNE 2016

## INTRODUCTION

Chairman Thornberry, Ranking Member Smith, and Members of the Committee, thank you for inviting us to discuss the Department of Defense (DoD) efforts in cyberspace. It is an honor to appear before you today and we appreciate the opportunity to explain the progress the Department is making to improve America’s cybersecurity posture.

We plan to focus our testimony on the approach the Department has taken in implementing DoD’s Cyber Strategy and how our approach to this mission space is advancing. Additionally, we will discuss our efforts to continue to develop, train, and equip our Cyber Mission Force (CMF). Finally, while we cannot discuss the particulars in this setting, we will also highlight how cyber capabilities support military operations within the context of Operation INHERENT RESOLVE. The Islamic State of Iraq and the Levant (ISIL) represents a serious and complex threat, and continues to use the internet to intimidate its enemies, recruit fighters, incite violence, and conduct or inspire attacks. Protecting the territory and people of the United States remains DoD’s highest priority, and cyber operations are one component in support of the whole-of-government effort against ISIL.

## THE CYBER THREAT LANDSCAPE

In addition to the threat posed by ISIL, we continue to face a diverse and persistent set of threats from state and non-state actors who probe and scan DoD networks for vulnerabilities. While the United States has benefited greatly from the increasingly wired and interconnected global landscape, cyber threats are increasing and evolving, posing greater risks to the networks and systems of the Department of Defense and other federal departments and agencies, our national critical infrastructure, and U.S. companies and interests.

As the recent indictment of Iranian cyber actors who infiltrated a hydroelectric dam in New York and launched attacks against the U.S. financial sector between late 2011 and mid-2013, as well as the attack on Sony Pictures Entertainment in 2014, demonstrates, the cyber threats to the United States and its infrastructure are real. If malicious cyber actors gain access to DoD networks, they can potentially manipulate information or software, destroy data, harm computers that host data, and even impair the functioning of systems that computers control. The successful intrusion into the Joint Staff's unclassified network demonstrates that despite our efforts, sophisticated actors can penetrate DoD systems. More broadly, the cyber incident involving Ukraine's power grid that led to power outages and damage to electrical control systems illustrates the broader impacts on society that cyberattacks can have. While DoD maintains and uses robust and unique cyber capabilities to defend our networks and the nation, often these measures alone are not sufficient. Securing systems and networks is everyone's responsibility – from the commander down to the individual and across the Federal Government – and requires a culture of cybersecurity.

Interagency discussions focus heavily on criminal activity in cyberspace, but nations in many ways still represent the gravest threats because of the skill and resources they can bring to bear. The states that we watch most closely in cyberspace remain Russia, China, Iran, and North Korea. Russia and China are both very capable cyber operators, while Iran and North Korea represent lesser, but still significant, challenges to U.S. interests. At DoD, we remain vigilant, and devote substantial resources and effort preparing for future threats that could be directed against the U.S. homeland, critical infrastructure that the Department relies on, and communication networks that we require to operate during a contingency.

## DOD STRATEGY AND MISSIONS

Since DoD’s Cyber Strategy was signed in April 2015, the Department has devoted considerable resources to implementing the goals and objectives outlined within the document. When Secretary Carter signed the Strategy, he directed the Department to focus its efforts on three primary missions in cyberspace: (1) defend DoD information networks to assure DoD missions, (2) defend the United States against cyberattacks of significant consequence, and (3) provide full-spectrum cyber options to support contingency plans and military operations.

In addition to DoD’s core missions in cyberspace, one of the Department’s key policy goals in cyberspace is to deter cyberattacks. DoD is supporting a comprehensive, whole-of-government cyber deterrence strategy to deter attacks on U.S. interests. This strategy will depend on the totality of U.S. actions, to include declaratory policy, overall defensive posture, effective response procedures, indications and warning capabilities, and the resiliency of U.S. networks and systems.

Fundamentally, however, deterrence is largely a function of perception, and DoD has three specific roles to play within a whole-of-government deterrence strategy. First, we seek to deny the adversary the ability to achieve the objectives of a cyberattack, so our adversary will believe any attack will be futile. We do this through strengthening our cyber defenses and reducing our attack surface. Second, we want to improve our resilience, so our adversary will perceive that even if any single attack is successful, we can reconstitute quickly so that their ultimate objective will not be achieved. The Department is already training to operate in a "cyber contested environment,” to demonstrate that we can continue our mission even while under cyberattack. Lastly, for deterrence to be effective, the adversary must believe that our ability to respond to an attack will result in unacceptable costs imposed on them. Costs may be imposed through a variety of mechanisms, including economic sanctions, diplomacy, law enforcement, and military action. Our task at the Department is to plan and prepare to conduct Title 10 military operations, including through cyberspace, to impose costs on the adversary.

**PROTECTING OUR NETWORKS**

Our primary mission remains the defense of the Department's information systems to assure the ability to conduct DoD missions; if these systems do not function, our national military power is at risk in all of the domains in which it operates. The Department's recent budget submission clearly reflects the high priority of this effort. Of the $6.8 billion of DoD's cyberspace budget request, $3.9 billion are designated for cyber security or cyber defense activities. This contributes to a broader $19 billion investment across the Administration on cybersecurity and in support of the Cybersecurity National Action Plan.

In order to secure its networks, the Department is pursuing multiple lines of effort to include the DoD Cybersecurity Discipline Plan and the DoD Cybersecurity Scorecard. These two initiatives mutually reinforce one another and ensure that cybersecurity becomes "commanders business" and receives direct leadership focus to address shortcomings and gaps. The Cybersecurity Discipline Plan focuses on strong authentication, device hardening, reducing the attack surface, and alignment to cybersecurity and computer network defense providers; the Scorecard measures the most important elements of the DoD Cybersecurity Discipline Plan. The data from the Scorecard is reviewed by the Secretary. Also, in March 2016, Secretary Carter launched the first cyber bug bounty program in the history of the federal government, "Hack the Pentagon," to reward vetted hackers who report bugs related to vulnerabilities or hacking exploits. This innovative initiative tested the Department's networks and engaged the hacker community to contribute to the security of the internet.

At the Command level, USCYBERCOM is working to harden and defend our networks. In addition to the DoD Chief Information Officer (CIO), who provides the technical standards and implementation of policy, USCYBERCOM works daily with the National Security Agency (NSA), the Defense Information Systems Agency (DISA), the Combatant Commands, and the military services to secure, operate, and defend DoD systems. Improving our collective cyber defenses is a whole-of-government and whole-of-nation endeavor that also requires close partnership with our allies.

## THE CYBER MISSION FORCE

The complete build of the Cyber Mission Force underpins DoD's primary missions in cyberspace and all our efforts in this domain. The heart of DoD's cyber capability – both offensive and defensive – lies with a dedicated professional cyber force. USCYBERCOM manpower reflects a true total force effort encompassing a robust active component along with both Guard and Reserve forces fully integrated at all echelons from USCYBERCOM headquarters to the tactical edge of our CMF.

Recruiting and retaining a talented cyber workforce is a top priority for Secretary Carter. Section 1107 of the Fiscal Year (FY) 2016 National Defense Authorization Act (NDAA) granted DoD the authority to establish a Title 10 Civilian Cyber Excepted Service Workforce to assist in carrying out the responsibilities of USCYBERCOM and the elements of the Military Departments supporting it. This step from Congress was an important and welcome step forward to manage our civilian cyber workforce, and will provide them the fulfilling career path and competitive pay that we need to keep our best employees.

Our Combat Mission Teams (CMTs) are on the cutting edge and operate with the combatant commands to support their missions, while National Mission Teams (NMTs) prepare to defend the nation's critical infrastructure from malicious cyber activity.  Cyber Protection Teams (CPTs) defend DoD Information Networks alongside DoD Computer Network Defense Service Providers.  The Department continues to build out DoD's 133 CMF teams, and the Services are actively working to support the achievement of full operational capability for the entire CMF by the end of FY18.  We have also begun to transition from focusing on "building the force" to monitoring more traditional "readiness" metrics, with all the CMF teams reporting their readiness within DoD reporting systems, like our warfighting units do.

The Cyber Mission Force gives USCYBERCOM the capacity to operate on a global scale.  The National Command Authority can call on CMF teams to bring cyberspace effects in support of global military operations.   Such work occurs daily, for instance, in the fight against ISIL, as Secretary Carter has discussed.  Portions of the CMF are executing cyber operations to make it more difficult for ISIL to plan or conduct attacks against Americans and our allies.  Cyber is a domain like air, sea, and land, and as we continue to conduct cyber operations in support of broader operations, like we are doing against ISIL, we expect to talk about it with increasing openness.

USCYBERCOM recently employed CPTs to respond to intrusions in DoD systems.  CPTs played an important role in remediating the Joint Staff's unclassified systems after an intrusion last year, and in correcting the misconfiguration the intruders had utilized.

Training the force for such missions is imperative. DoD regularly participates in exercises that explore and push to improve policies and processes for providing assistance to DoD components as well as civil authorities in the context of a cyberattack. In these exercises, such as the Department of Energy's GridEx and ClearPath series, and USCYBERCOM's CYBER GUARD Exercise, which took place last week, DoD works with a wide range of interagency, state, local, and industry participants to understand and improve planning for scenarios to provide emergency assistance cooperatively with DHS, the FBI and the Sector-Specific Agencies identified in Presidential Policy Directive 21. These exercises have helped inform DoD's thinking regarding what kind of support we might be asked to provide and have also been an important tool for educating industry about what the federal government, including DoD, might provide in a crisis. The support for CYBER GUARD from our public and private partners has been positive. Exercises like CYBER GUARD allow senior policymakers to observe the types of issues seen in real cyberattacks, and helps us generate lessons learned that should save the federal government precious time and effort in crafting its response.

In addition to exercises, the Department continues to advance its thinking and organization on the topic of cyber test and training ranges. The primary purpose of cyber test capabilities and ranges is to enable the development, acquisition, and sustainment of DoD resilient systems, while training ranges are critical to mission rehearsal and sustainment of DoD's Cyber Mission Forces. The FY 2015 NDAA, Section 1633, directed that DoD establish Executive Agents for a Cyber Training Range and a Cyber Test and Evaluation Range. This legislation was instrumental in helping the Department establish roles and responsibilities in the area of training for the CMF – critical to the readiness of our forces - and in NDAA FY 2016, this work was leveraged to support the designation of the Executive Agent for Section 1645, Persistent Training Environment (PTE). PTE is critical to the collective training of the CMF and budget cuts to this training capability place the readiness of our forces at serious risk.

## CONCLUSION

The Department is committed to the security and resiliency of our networks and to defending the U.S. homeland and interests from attacks of significant consequence that may occur in cyberspace. We have undertaken comprehensive efforts, both unilaterally and in concert with our interagency partners, allies, and the private sector to improve our nation's cybersecurity posture and to ensure that DoD has the ability to operate in any environment at any time. Our relationship with Congress is absolutely critical to everything the Department is doing. To that end, I am grateful for the committee's interest in these issues, and I look forward to your questions.