

ASD Creedon Testimony
HASC on Emerging Threats and Capabilities
March 20, 2012

Introduction

Thank you, Mr. Chairman and Ranking Member Langevin, for inviting the Department of Defense (DoD) to discuss our strategies and activities for addressing cyberspace challenges and opportunities. I am pleased to appear here today with Ms. Teri Takai, the DoD CIO, and General Keith Alexander, the Commander of U.S. Cyber Command. We are all here on behalf of the men and women of the Department who commit themselves every day to ensuring the safety of the United States, both at home and abroad.

Today I intend to present a brief overview of the Department's efforts in cyberspace, and I will provide an update on the implementation of the *Defense Strategy for Operating in Cyberspace* and the progress we have made in meeting the *Quadrennial Defense Review* and *Strategic Guidance* goals of operating effectively in cyberspace.

DoD continues to develop effective strategies for ensuring that the United States is prepared for all cyber contingencies across the entire spectrum from peace to crisis to war. Importantly, during these times of fiscal constraint, DoD is taking advantage of the efficiencies provided by advances in information technology.

Almost every feature of modern life now requires access to information infrastructure and DoD is no different. We maintain over 15,000 networks or enclaves and seven million computing devices in installations around the globe. The networks upon which the DoD relies represent both opportunities and challenges.

Looking forward, Secretary Panetta addressed the issue of cyber in his testimony to the House Armed Services Committee in October 2011 when he stated, “We continue to have to confront cyber attacks and the increasing number of those attacks that threaten us every day.” We are considering increased spending on cyber over the next few years, even as we are planning significant cuts in other areas. Some particular areas where we may desire increases in the cyber budget might include:

- Increasing situational awareness tools and capabilities to monitor the security posture of DoD networks;
- Strengthening our ability to test capabilities and to operate effectively in a degraded environment; and
- Improving DoD support to the cybersecurity of the Defense Industrial Base and U.S. critical infrastructure, as appropriate.

Threats

These investments are critically important; they set the foundation for the Department’s ability to face and defend against an ever-growing threat from malicious cyber actors. Whereas that threat was once the province of lone-wolf hackers, today, our nation, our businesses, and even our individual citizens are constantly targeted and exploited by an increasingly sophisticated set of actors. We believe the costs of these intrusions run into the billions of dollars annually and pose a clear threat to our economy and our security. Further, we are increasingly concerned about the threat to our Defense Industrial Base and the nation’s critical infrastructure. We have seen the loss of significant amounts of intellectual property and sensitive Defense information that resides on or transits Defense Industrial Base systems. This

loss of key intellectual property has the potential to give an adversary leap-ahead technology to achieve parity with some of our most sensitive capabilities. As the recent report from the National Counterintelligence Executive shows, China conducts cyber-enabled economic espionage in order to shore up and support its military industries, thereby undermining the U.S. competitive edge in key technologies.

U.S critical infrastructure is increasingly vulnerable to cyber threats. DoD depends upon this infrastructure, including the electric grid, the telecommunications infrastructure, and key transportation systems, in order to function. Unless we as a nation do more to protect critical infrastructure assets and intellectual property, it is likely only a matter of time before we suffer a crippling blow that will greatly diminish DoD's ability to conduct our missions. DoD is ready to assist in this effort.

DoD's Actions

The Department has been working around the clock, often in close coordination with the Department of Homeland Security and other agencies, to protect the nation from these threats. Last July, DoD released the *Defense Strategy for Operating in Cyberspace* (DSOC). This strategy was a significant milestone for the Department because it was the first comprehensive strategy to address this new operational domain. The DSOC built upon the President's *National Security Strategy*, the *International Strategy for Cyberspace*, and the Department's *Quadrennial Defense Review*. The DSOC guides the Department's military, business, and intelligence activities in cyberspace to support of U.S. national security. Through five strategic initiatives, the DSOC lays out a framework to capitalize on the opportunities and address the threats created by cyberspace.

- First, DoD will treat cyberspace as an operational domain in order to organize, train, and equip our forces.
- Second, DoD will employ new operating concepts in order to protect DoD networks and systems.
- Third, DoD will partner with other departments and agencies, as well as the private sector, in order to enable a whole-of-government approach to cybersecurity.
- Fourth, DoD will build robust relationships with allies and international partners to strengthen our collective cybersecurity.
- Fifth and finally, DoD will leverage the nation's ingenuity by making more effective use of the cyber workforce and fostering rapid technological innovation.

DoD has made strides in each of these areas since the strategy was introduced nine months ago and established a governance body to manage the implementation of those initiatives. Co-chaired by the Under Secretary of Defense for Policy and the Director for Operations for the Joint Staff, the Cyber Integration Group assigns actions to appropriate components across OSD, the Joint Staff, the Services, the Combatant Commands, the Defense Cyber Crime Center, the National Security Agency, and the office of the Chief Information Officer. The accomplishments of this group attest to the progress we have made in addressing many of the issues regarding the new operational domain of cyberspace.

The Department is working with the Administration to update cyberspace operations policy, determine how we can better defend our critical infrastructure and intellectual property, and respond to advanced persistent threats. While we are responsible for protecting DoD's information systems and networks from cyber threats, the protection of infrastructure critical to national security requires the entire government's effort and extends to privately held

infrastructure owners. We are working closely with the Executive Branch Departments and Agencies on this significant challenge. Our recent Defense Industrial Base Cyber Pilot demonstrated that DoD could enhance the cybersecurity of Defense Industrial Base companies through a public-private cyber threat information sharing program.

Further, we are integrating cyber effects into our operational planning and addressing the policy issues constraining activity in this area. The Department is currently conducting a thorough review of the existing rules of engagement for cyberspace. We are also working closely with the Joint Staff on the implementation of a transitional command and control model for cyberspace operations. This interim framework will standardize existing organizational structures and command relationships across the Department to provide the full spectrum of cyberspace capabilities in response to the requirements of the President. The Joint Staff is also in the process of developing a Joint Publication for Cyberspace Operations. Although cyberspace operational doctrine already exists in various current publications, this will be the Department's first Joint Publication focused solely on cyberspace operations.

Also in line with our strategy and in accordance with the President's *International Strategy for Cyberspace*, DoD is developing a range of capabilities to protect the nation from our adversaries. The purpose of these capabilities is to provide the President with a full range of options to use in defending and securing our Nation in concert with the other elements of power we can bring to bear.

Within the U.S. government, DoD also works very closely with our colleagues in the Departments of Homeland Security, Justice, State, Treasury, Commerce, and others. Although DoD maintains robust and unique cyber capabilities that we use to defend our networks and the nation, we strongly believe in a whole-of-government approach to cybersecurity. As such, we

fully support the Department of Homeland Security's role coordinating the overall national effort to enhance the cybersecurity of U.S. critical infrastructure.

One example of interagency collaboration is the former Defense Industrial Base Cyber Pilot, now known as the Joint Cybersecurity Services Pilot. Based initially on the Defense Industrial Base Cybersecurity and Information Assurance Program that is run by the DoD Chief Information Officer, DoD and Homeland Security established an information sharing construct with Commercial Service Providers to provide managed security services enhanced by government threat information to Defense Industrial Base companies. In partnership with Homeland Security, we are working together on plans make it a permanent program for the Defense Industrial Base.

Finally, we are working closely with our interagency partners to address the vulnerabilities represented by the supply chain of critical equipment upon which our networks and systems rely. DoD serves as a co-lead on a supply chain risk management task force that was established a year ago and we are making progress in addressing the requirement for a secure and trusted manufacturing environment.

Beyond the U.S. government, DoD is also working with our interagency partners and the private sector to improve security and foster innovation, while ensuring an open, accessible and private sector-owned Internet. We understand that building strong partnerships with industry is essential to our collective security. An important initiative in this area is the Enduring Security Framework, which provides a mechanism for Homeland Security, DoD, and the Director of National Intelligence to work with key industry leaders on cybersecurity issues that affect both the private sector and defense and government networks.

On the international front, DoD is pursuing both bilateral and multilateral engagements. First, we are collaborating with our close allies such as the United Kingdom, Australia, Canada, Japan, and the North Atlantic Treaty Organization on improving international cybersecurity. We are also working closely with the Department of State to develop international norms of behavior that will serve to guide our international partnerships. If international norms of behavior in cyberspace could be achieved, adherence to such norms would bring a level of predictability to state conduct and help prevent the misunderstandings that could lead to conflict. In addition, DoD also participates and interacts with the various Internet governance institutions to ensure that the Internet remains open, interoperable, secure, and reliable.

In addition to the increasing threats we face through cyberspace, one of the challenges is the lack of clear authorities for providing for the cybersecurity of U.S. critical infrastructure. Although the Department does not require any additional authorities in cyberspace for Defense missions, we do support providing additional authorities to the Department of Homeland Security, including the authority to establish, in consultation with the other agencies of the government, risk-performance standards for core critical information infrastructure to ensure a baseline level of security

Another challenge is to balance the nation's need for cybersecurity with privacy and civil liberties. In this area, DoD is committed to focusing on external actors while ensuring the privacy and civil liberties of our citizens in our efforts to support the cybersecurity of U.S. critical infrastructure.

Conclusion

Thank you for this opportunity to describe some of the opportunities and challenges that DoD faces in cyberspace. These lines of effort represent significant investments in our nation's defense and reflect the high priority that Secretary Panetta places on cybersecurity. DoD is working hard to ensure our nation's security, but there is still more work to be done.

We fully support Congressional efforts to provide the Department of Homeland Security, as our partner and domestic lead for cybersecurity, with the authorities and resources it needs. We also believe that Homeland Security should have the authority to designate core critical infrastructure and establish baseline risk-based performance standards for cybersecurity. Additionally, we must do more to encourage information sharing in a way that maintains the Administration's focus on the maintenance of privacy and civil liberties. These reforms would go a long way to keeping our nation ahead of the evolving threat while protecting our basic values. With the help of and partnership with Congress, DoD is working hard to protect our nation and to provide the necessary capabilities to keep our country safe.