Statement for the Record

The Honorable Eric Rosenbach

Assistant Secretary for Homeland Defense and Global Security and Principal Cyber Advisor to the Secretary of Defense

U.S. Department of Defense

Before the

U.S. Senate Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities

Chairman Fischer, Ranking Member Nelson, and members of the Subcommittee, thank you for inviting me to discuss Department of Defense (DoD) efforts in cyberspace. It is my honor to appear today with my colleague from U.S. Cyber Command, Lieutenant General McLaughlin. Cybersecurity is an increasingly urgent and important topic in today's interconnected world, and I appreciate the opportunity to explain the Department's mission in this space and how we continue to improve America's cybersecurity posture.

With respect to cyberspace, the Department of Defense continues to focus on its three vital missions: (1) defending DoD information networks to assure DoD missions, (2) defending the nation against cyberattacks of significant consequence, and (3) providing cyber support to contingency plans and operations. Today, we face diverse and persistent threats in cyberspace that cannot be defeated through the efforts of any single organization. Although DoD maintains robust and unique cyber capabilities that we use to defend our networks and the nation, we must continue to work closely with our partners in the federal government, the private sector, and in countries around the world to ensure we have the necessary strategies, policies, capabilities, and workforce in place to succeed.

The Cyber Threat Landscape

We live in a wired world, and despite the convenience that connectivity brings, it also makes robust cybersecurity more important than ever. State and non-state actors are conducting cyber operations for a variety of reasons, expanding their capabilities, and targeting the public and private networks of the United States, its allies, and partners. These cyber threats continue to increase and evolve, posing greater risks to the networks and systems of the Department of Defense, our national critical infrastructure, and U.S. companies and interests.

External actors probe and scan DoD networks for vulnerabilities millions of times each day, and over one hundred foreign intelligence agencies continually attempt to infiltrate DoD networks. Unfortunately, some incursions – by both state and non-state entities – have succeeded.

Malicious actors are also targeting U.S. companies. At the end of last year, North Korean actors attacked Sony Pictures Entertainment in the most destructive cyberattack against the United States to date. North Korea destroyed many of Sony's computer systems, released personal and proprietary information on the Internet, and subsequently threatened physical violence in retaliation for releasing a film of which the regime disapproves.

Cyberattacks also pose a serious threat to networks and systems of critical infrastructure. The Department of Defense relies on U.S. critical infrastructure to perform its current and future missions. Intrusions into that infrastructure may provide persistent access for potential malicious cyber operations that could disrupt or destroy critical systems in a time of crisis. Because of these severe consequences, DoD is working with our partners in the interagency and private sector to ensure these systems are better protected.

At DoD, we are also increasingly concerned about the cyber threat to the companies in our Defense Industrial Base. We have seen the loss of significant amounts of intellectual property and sensitive DoD information that resides on or transits Defense Industrial Base systems. This

loss of key intellectual property has the potential to hurt our companies and U.S. economic growth, but also enables adversaries to more easily achieve technological parity with us.

In light of these evolving threats, DoD is committed to 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, DoD must develop cyber capabilities to *deny* a potential attack from achieving its desired effect. If our adversaries perceive that they are not going to succeed in conducting an attack they will be less inclined to act. Second, the United States must increase the *cost* of executing a cyberattack. In that regard, DoD must be able to provide the President with options to respond to cyberattacks on the United States if required, through cyber or other means. As the President has said, the United States reserves the right to respond to cyberattacks at a time, in a manner, and in a place of our choosing. Finally, we must ensure our systems are *resilient,* and able to withstand and recover quickly from any potential attack on our own networks. Within DoD, it is our responsibility to make our own systems resilient. Nationally, we support other agencies of the government, like DHS and the National Institute of Standards and Technology, in fostering effective resiliency measures for the country as a whole.

To support our deterrence posture, DoD is investing significantly in our Cyber Mission Force to conduct cyber operations. Underpinning the Cyber Mission Force, we have built robust intelligence and warning capabilities to reduce anonymity in cyberspace and identify malicious actors' tactics, techniques, and procedures. Our attribution capabilities have increased significantly in recent years, and we will continue to work closely with the intelligence and law enforcement communities to maintain effective attribution capabilities.

DoD's Evolving Cyber Strategy and the Future Cyber Workforce

As I have said, the Department of Defense has 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. U.S. Cyber Command (USCYBERCOM), as a sub-unified command to U.S. Strategic Command (USSTRATCOM), is responsible for defending DoD networks and defending the nation from cyber threats, and works in partnership with the combatant commands to conduct full-spectrum cyber operations.

To carry out these missions, we are building the Cyber Mission Force and equipping it with the appropriate tools and infrastructure to operate in cyberspace. Once fully manned, trained, and equipped in Fiscal Year 2018, these 133 teams will execute USCYBERCOM's three primary missions with nearly 6,200 military and civilian personnel.

As we continue to strengthen the Cyber Mission Force, we recognize the need to incorporate the strengths and skills inherent within our Reserve and National Guard forces. Each Service, therefore, has developed Reserve Component integration strategies that embrace Active Component capabilities in the cyberspace domain and leverage the Reserve and National Guard strengths from the private sector. Up to 2,000 Reserve and National Guard personnel will also support the Cyber Mission Force by allowing DoD to surge cyber forces in a crisis. When called upon, these surge forces will serve as a robust DoD-trained force to help defend national critical infrastructure.

As Secretary Carter has said several times in the last month, the development of a cadre of cyber experts – both in and out of uniform -- is essential to the future effectiveness of U.S. cyber capabilities, and we are committed to ensuring the workforce for the cyber domain is as world class as the personnel in other warfighting domains. To that end, we are developing and retaining a workforce of highly skilled cyber security specialists with a range of operational and intelligence skill sets. This cyber workforce must include the most talented experts in both the uniformed and civilian workforce, as well as a close partnership with the private sector. Achieving robust capabilities will require long-term planning and investment to ensure that a pipeline of cyber security talent is available to benefit the Department of Defense and the nation as a whole.

Over the past several years, DoD's approach toward cyberspace has continued to evolve and mature. As such, the Department is in the process of finalizing a new, updated strategy, which will guide DoD's activities in cyberspace in defense and support of U.S. national interests. Once approved by the Secretary, we plan to conduct a series of briefings and discussions with Members of Congress and their staffs. This strategy builds upon our previous cyber strategy from 2011, the national security missions and objectives of the *2014 National Security Strategy*, the *2014 Quadrennial Defense Review*, and the *2011 International Strategy for Cyberspace*.

Building Strong Partnerships

Successfully executing our missions in cyberspace requires a whole-of-government and whole-of-nation approach. DoD continues to work with our partners in other federal Departments and agencies, the private sector, and countries around the world to address the shared challenges we face. We work particularly closely with our partners in the Department of Homeland Security and Department of Justice to ensure collaboration in cyber operations and information sharing across the federal government, and we have seen tremendous advancement in our ability to work as a single, unified team.

Additionally, Secretary Carter has placed a particular emphasis on partnering with the private sector. We need to be more creative in finding ways to leverage the private sector's unique capabilities and innovative technologies. The Department does not have all the answers, and working with industry will be critical to ensuring our technical military advantage in the future. We are examining ways to expand our collaboration with industry and developing incentives and pathways to bring more cyber expertise into the Department.

Finally, our relationship with Congress is absolutely critical. As the President has said many times, Congressional action is vital to addressing cyber threats. I appreciate the early steps taken during this session to build consensus on information sharing legislation, and await progress on other key provisions, such as data breach and cyber criminal provisions, included in the President's legislative proposal submitted earlier this year.

Conclusion

Cyber threats are real, serious, and urgent, and we can only overcome them with a cohesive, whole-of-government approach. We have made significant strides, but there is still more work to be done. I look forward to working with this Committee and the Congress to ensure that DoD has the necessary capabilities to keep our country safe and our forces strong. Thank you again for the attention you are giving to this urgent matter. I look forward to your questions.