STATEMENT OF

MR. KENNETH RAPUANO

ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE

AND GLOBAL SECURITY

AND PRINCIPAL CYBER ADVISOR

TESTIMONY BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

APRIL 11, 2018

Thank you Chairman Stefanik, Ranking Member Langevin, and Members of the Committee. It is an honor to appear before you alongside Admiral Rogers, Commander of U.S. Cyber Command, to discuss the Department of Defense's (DoD's) priorities in cyberspace. I am testifying today in my roles as Assistant Secretary of Defense for Homeland Defense and Global Security and as Principal Cyber Advisor to the Secretary of Defense. In these roles, I oversee the development and implementation of the Department's cyber strategy and policy with regard to cyberspace; lead the Department's interagency cyber coordination efforts; advise the Secretary and the Deputy Secretary on cyberspace activities; and ensure that the Department's cyber forces and capabilities are integrated across the Joint Force to support the missions assigned by the President to the Secretary of Defense.

The United States faces a complex global security environment characterized by disorder and challenges to the free and open international system. We are in the midst of a long-term strategic competition with two revisionist powers, China and Russia, who seek to shape a world consistent with their authoritarian model. At the same time, U.S. military superiority is increasingly contested in every operating domain by competitors who are fielding capabilities aimed at the battle networks and

operational concepts which underpin Joint Force power projection. Finally, the arrival of the cyber era means that the United States homeland is no longer a sanctuary. State and non-state actors now have the ability to carry out malicious cyberspace activity against U.S. political, economic, and security interests without ever having to cross our borders.

The Department's primary mission is to provide combat-credible military forces to deter and win wars and protect the security of the United States. To that end, DoD cyber forces must ensure that the Joint Force can operate in a cyber-contested environment, support Joint Force lethality with cyber capabilities, and deter or defeat strategic cyber-attacks against the homeland.

Accomplishing these missions requires DoD to be ready to fight in and through cyberspace against a great-power competitor. The Department must maintain the ability to gain access to foreign networks and systems, collect information, and, when necessary, deliver effects in and through the cyberspace domain. The 2018 National Defense Strategy provides a prioritization framework for cyber missions that amplifies its three themes: increasing lethality, strengthening alliances, and reforming the Department's practices. Our end goal is the successful integration of

cyber operations across the Joint Force and throughout all the Department's core missions rather than the sidelining of those capabilities as a niche for a specialized cadre of technical experts.

Cyber security is inherently a team sport. Cybersecurity experts estimate that some 90 percent of cyber-attacks could be defeated by better implementation of basic cyber hygiene practices and best practice sharing. Through basic cyber hygiene and information sharing across the government and private sector, we can drastically decrease the opportunities for our adversaries to hold us at risk. In turn, as we increasingly spend less time countering malicious cyber activity directed against us, we commit more time and resources to developing capabilities to hold our adversaries at risk.

Defending the Joint Force

Defending DoD networks, systems, infrastructure, and information is essential to ensuring the Joint Force can operate in a cyber-contested environment. A successful defense requires the Department to be able to operate in our adversary's cyber-attack infrastructure to preempt, blunt, or halt attacks. DoD also protects its systems and networks by implementing cyber resiliency measures such as hardening against cyber-attacks and

ensuring mitigations have been developed that allow continued functioning when a cyber-attack does occur. If and when the Department detects malicious cyber activity within its networks, DoD's rapid-response capabilities can be brought to bear to secure its networks and systems by halting the cyber adversaries.

Defending the Department's networks also requires identifying and mitigating our own vulnerabilities. As a Department, we recognize that we rely heavily on cyber-enabled critical infrastructure to conduct our core missions and appreciate congressional efforts to expand and strengthen vulnerability identification programs. We are improving and broadening our risk-management framework to assess threats across the Joint Force and allow us to prioritize the mitigation and remediation of our most critical vulnerabilities. We are also moving forward to assess and readdress major weapon systems and critical infrastructure vulnerabilities as mandated by Section 1647 of the National Defense Authorization Act for Fiscal Year 2016 and Section 1650 of the National Defense Authorization Act for Fiscal Year 2017.

Protecting DoD information residing in the Defense Industrial Base (DIB) is critical to enabling Joint Force military overmatch. The wartime

cybersecurity of our systems and networks will mean little if the qualitative advantage of our weapons platforms has been eroded during peacetime by the exfiltration of sensitive military information. The Department must more effectively compete with and challenge cyber actors who are stealing United States defense information by being more proactive and creative in how we leverage counterintelligence authorities to combat information theft.

Ensuring that DoD contractors maintain adequate cybersecurity standards is also critical to protecting the Department's information. In October 2016, we updated the Defense Federal Acquisition Regulation Supplement (DFARS) to require contractors to provide "adequate security" for covered defense information that is processed, stored, or transmitted on the contractor's internal information system or network. We are continuing to evaluate our mandated cybersecurity standards for DoD contractors and working to protect our information outside of Department networks.

Beyond the DIB, we are advancing our understanding of the degree to which Joint Force operations are reliant on civilian defense critical infrastructure (DCI). Much of our warfighting capabilities are dependent on an array of municipal utilities, national utilities, private telecommunications companies, transportation networks, and other assets that are not

connected to our networks and over which we have limited visibility and control. DoD's Mission Assurance process provides a way for us to systematically and thoroughly examine these dependencies and the risks to our military and civilian infrastructures, networks, and systems. We are working to prioritize civilian DCI assets by their criticality to the Department's priority missions so that we can mitigate those risks and build resiliency across all domains, including cyberspace.

Enhancing Joint Force Lethality

DoD is moving to normalize the consideration of cyber capabilities throughout Joint Force operations and contingency planning in order to fully integrate maneuver in the cyberspace domain with maneuver in the physical domains. Cyber capabilities provide commanders with unique tools that have different characteristics than conventional weapons. We must experiment now with innovative ways to pair cyber with other military capabilities to ensure that the Joint Force remains at the forefront of operational proficiency in this new warfighting domain.

Defending the Nation

Defending the nation is a core mission of the Department of Defense and just as we develop military forces, capabilities, and plans to project

power to meet threats from land, air, and sea, we must also be prepared to do so in cyberspace. In this way, the Department is focused on preparations to defend the United States by halting or degrading strategic cyber-attacks using cyber effects operations, as well as developing a range of response options. Additionally, we seek to leverage the Department's extensive information collection mechanisms to provide timely indicators and warnings (I&W) to public and private network and system owners and operators both broadly to enhance our collective preparedness against cyber threats, as well as specifically, so that they can raise their cybersecurity posture if an attack is imminent. DoD runs three of the six Federal cybersecurity centers, which participate in the Enhanced Shared Situational Awareness Initiative (ESSA). I&W information is a two-way street. We want to ensure mechanisms are in place for public and private sector partners to inform us of malicious cyber activity taking place in their networks and systems so that we can potentially address the threat at its source.

Deterrence in Cyberspace

DoD uses "cyber deterrence" to refer to actions taken to convince adversaries not to conduct destructive or destabilizing malicious cyber

activity against the United States However, to date, the United States' limited responses and inconsistent messaging have been ineffective at halting cyber behavior we consider unacceptable. This is challenging – absolute deterrence – or a complete elimination of all malicious cyber activity is unlikely, since cyber weapons are quite unlike nuclear weapons; however, more can and should be done to strengthen our deterrence posture.

The President recognized the importance of a stronger deterrence posture in the 2017 Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," which directed the development of a whole of government approach to deterrence, which was just recently completed. Consistent with these recommendations, and the 2017 report from the Defense Science Board Task Force on Cyber Deterrence, we are implementing a range of actions to improve our ability to deter our adversaries in cyberspace. First, the Department is working alongside other U.S. departments and agencies to develop tailored deterrence plans aligned against specific threats and types of malicious cyber activity. In this way, DoD will contribute to a national-level effort, driving planning and assessment activities for such adversary-focused plans, as well as refining military options, forces, and authorities

that can be leveraged to advance our national interests and contribute to stability and security in cyberspace. Second, the Department is strengthening our ability to operate in a cyber-contested environment, as previously discussed, through ongoing cyber vulnerability assessments of major weapon systems and critical infrastructure and through the effective use of Combatant Command exercises and wargames. The results of these cyber vulnerability assessments, exercises, and wargames will inform risk-based decisions on the most effective way to improve the capability of DoD forces to operate in a cyber-contested environment. Lastly, the Department's Fiscal Year 2019 budget supports U.S. Cyber Command's role to train and equip the Cyber Mission Force with acquisition efforts focused on the four capability areas of: Joint Access Platforms, Joint Tools, Joint Analytics, and Joint Common Services. These investments in foundational capabilities combined with the broader U.S. government's efforts to enhance the cyber security of the most vital U.S. critical infrastructure will substantially bolster the U.S. cyber deterrence posture.

I acknowledge that the Department's report on deterrence strategy to the Congress is long overdue. I continue to work with Department leaders and interagency partners to refine and enhance our deterrence posture and

to present the comprehensive and substantive response your questions deserve.

Building a Cyber Force

One of the Department's most significant cyber accomplishments has been the creation of the Cyber Mission Force (CMF). With more than 6,000 soldiers, sailors, airmen, Marines, and civilians the CMF's ranks include some of the brightest and most talented men and women serving in in the Department. The force is on schedule to complete full force generation before the end of the fiscal year, reflecting the successful completion of a multi-year train-and-equip effort. The current CMF benefits from significant contributions from the Reserve Components, which are being further developed in the near future. We are leveraging the Total Force to meet the Department's needs while promoting strong relationships with state and local authorities that allow our cyber warriors to maintain their ties with their communities even as they contribute to the defense of the Nation.

Reaching completion of the force generation phase is an important step for the CMF and is a testament to the hard work of the Military Departments that have built these forces. As we approach this milestone

before the end of this fiscal year, our focus has increasingly shifted to enhancing readiness with an emphasis on training and capability development. Military operations in cyberspace continue to provide U.S. forces with operational experience as well as insights into the command and control capabilities required to effectively conduct integrated cyber operations. Specific activities aligned with training the CMF include the acquisition of a Persistent Cyber Training Environment (PCTE) and the effective leveraging of existing Joint and Service cyber training capabilities. In addition, we are procuring new capabilities to be more ready in and through cyberspace. With continued congressional support, we will provide our Nation with an agile and war-winning cyber force.

The Department is also moving forward with developing the civilian cyber workforce with the September 2017 launch of the Cyber Excepted Service (CES), an enterprise-wide approach to managing the civilian cyber workforce. CES provides the Department with the agility and flexibility to identify, recruit, develop, and retain the very best cyber professionals. It helps the Department streamline hiring procedures to fill critical cyber positions quickly across the enterprise by providing hiring managers with more options for sourcing candidates and allowing them to offer more competitive compensation packages. I thank you and the other members

of Congress who have supported the efforts to provide the Department the hiring and managing authorities and the means to provide the world's best training to our cyber forces. We are monitoring these programs closely to ensure that we have the right mix of tools available to cultivate the workforce necessary for this 21st Century domain and we will report back to you on the effectiveness of our efforts.

Allies and Partners

The cybersecurity efforts of our allies and partners are critical to protecting ourselves from malicious cyberattacks. By establishing and cultivating international partnerships, the Department increases its capacity to detect, monitor, prevent, and defeat threats in cyberspace while working to ensure that our allies and partners develop and build strong cyber defense capabilities. Security cooperation activities in general, and cybersecurity cooperation activities in particular, provide an opportunity for the United States and the Department to improve and leverage the cyber capabilities and capacity of our allies and partners so they are able to help us shape the strategic environment in favor of U.S. national objectives.

Working with our allies and partners is also critical to establishing and enforcing responsible state behavior in cyberspace, giving strength to

shared rules of the road for stability and security in cyberspace. We are more effective when we stand shoulder to shoulder with our friends when calling to account those who act maliciously and recklessly by attacking the interconnected information and infrastructure that makes up cyberspace. The Department's security cooperation authorities will be helpful in developing the cyber capabilities of our allies and partners so that they are more effective at protecting their systems and engaging alongside us against our common adversaries. Although norms are unlikely to restrain the most malicious, persistent adversaries in cyberspace, they provide standards for responsible states, giving context to justified proportional response. Standing together with our like-minded allies and partners, we can increase the costs to those adversaries insisting on continuing malicious cyber activities that fall outside the norms of acceptable behavior.

Reforming Business Practices

The Department has been justly criticized for a bureaucratic culture that often prioritizes exacting thoroughness and minimizing risk over speed and innovation. We are optimized to deliver exquisite solutions developed over lengthy periods of time rather than immediate, perhaps imperfect solutions that can be improved iteratively. Our current approach is

particularly problematic in the cyberspace domain, where the most successful technology companies have adopted development models that revolve around rapid prototyping and rapid deployment followed by frequent and incremental updates. The Department is committed to ensuring that our cyber forces are able to leverage capability development processes that can deliver effective results in a timely manner. One of our efforts, outlined in Section 1642 of the National Defense Authorization Act for Fiscal Year 2018, is to ensure our cyber acquisition practices are as streamlined, agile, and efficient as possible in order to deliver the right tools rapidly to our warfighters.

Organizing for Success

U.S. Cyber Command has been given Service-like responsibilities that will allow it to acquire cyber-unique equipment and technology rapidly and to train its people to meet the latest threats. This is absolutely critical for an agile command responsible for maintaining the Joint Force's advantages in cyberspace. This Command is now functioning as an operational command while supporting other Combatant Commands by providing cyber operational planning and cyber effects. We can be very proud of the men and women who have worked tirelessly to make this

happen. I will continue to work closely with Admiral Rogers and, assuming confirmation Lieutenant General Nakasone, as U.S. Cyber Command approaches full operational capability to ensure that it has the powerful advocate it needs to continue its success.

The Department is developing the organization, processes, and procedures that will support the command as it becomes more mature and capable. The Department is developing options to meet the intent of Sections 902 and 923 of the National Defense Authorization Act for Fiscal Year 2017 (NDAA for FY 2017) and Sections 909, 1635, and 1637 of the NDAA for FY 2018. We continue to refine these options by assessing the Department's missions in and through cyberspace, considering the future environment, and analyzing the benefits and risks to optimize roles and responsibilities to ensure that the Department is best postured for this challenging and rapidly changing domain of warfare. I look forward to working with you and other members to structure the Department's approach to provide the appropriate military department secretary-like oversight and ensure that adequate guidance and support are provided to the newly elevated command.

Conclusion

I thank the subcommittee members for their continuing support of the Department's efforts to develop the cyber capabilities and capacity we need to adjust to the changing character of conflict. The people in our cyber community are the best in the world and I am honored to serve with them. The Department is committed to approaching the development of our cyber capabilities with the sense of urgency warranted by the gravity of threats we face. We have undertaken comprehensive efforts in concert with our interagency allies, partners, and the private sector to improve the Department's cybersecurity posture and to ensure that we have the ability to operate in any domain, at any time, and against any adversary. Our strong relationship with Congress has been a critical component of our success and will remain vital as we continue our work to ensure the Department's cyber forces are prepared to compete, deter, and win against any opponent. To that end, I am grateful for Congress's strong support and particularly this subcommittee's interest in these issues, and I look forward to your questions.