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

MARCH 13, 2019

Thank you Chairman Langevin, Ranking Member Stefanik, and Members of the Committee. I am pleased to be here with General Nakasone, Commander of U.S. Cyber Command (USCYBERCOM), to report on the significant progress the Department of Defense (DoD) has made over the last year in regard to cyber strategy and operations. I am testifying today in both my roles as Assistant Secretary of Defense for Homeland Defense and Global Security, and as Principal Cyber Advisor to the Secretary of Defense. I am responsible for advising the Secretary and the Deputy Secretary on cyberspace activities and the development and implementation of the Department's cyber strategy and policy with regard to cyberspace; leading our interagency coordination of our cyber efforts; and ensuring the integration of cyber capabilities across the Joint Force in support of the President and Secretary of Defense.

Threats and Strategic Objectives

Over the last year, the Department has made great strides in articulating its objectives for cyberspace, aligning the necessary resources to accomplish those objectives, and executing operations. To that end, the Administration has published a new, more proactive strategy for cyberspace, and is moving forward with implementation of that strategy using the first-ever Cyber Posture Review (CPR) and the elevation of USCYBERCOM. Our new approach has been enabled by the issuance of new Presidential guidance on cyberspace authorities, and legislation complementing the President's authority, that directs appropriate action in cyberspace against certain adversaries to disrupt, defeat, and deter active, systemic, and ongoing campaigns against the Government or people of the United States. Recent legislation also clarifies that certain cyberspace operations are traditional military activities. We leveraged all of these tools last year as we worked with our partners to ensure the security of the 2018 U.S. midterm elections.

We are continuing to gather and apply the lessons we have learned to defend the Nation from cyber threats.

This matter is urgent. The DoD Cyber Strategy makes clear that the ongoing campaigns of malicious cyber activity conducted by states like China and Russia are a strategic threat. Although our conventional military superiority is deterring these competitors from challenging the United States directly, our adversaries are increasingly resorting to malign activities in and through cyberspace to undermine U.S. security and prosperity. Their objective is to win without going to war. To achieve that goal, our competitors are conducting long-term, strategically focused campaigns in and through cyberspace that include stealing sensitive DoD information to undermine our military advantages, infiltrating our critical infrastructure so they can hold it at risk during a crisis or confrontation, and, in conjunction with activities in other domains, conducting influence operations targeting the American public.

Although the consequences of any single intrusion or action may be limited, in the aggregate these cyber campaigns are a strategic threat to the United States. Coordinated malicious cyber activity threatens our prosperity, our democratic institutions, and our national security, including by eroding our military advantage should a conflict occur.

For this reason, the DoD Cyber Strategy makes clear that the Department must embrace a proactive and assertive approach during day-to-day competition to deter, disrupt, and defeat these threats. The Department's networks and systems must be made so secure, resilient, and well-defended that we can be assured that the Joint Force will be able to execute its critical missions. During wartime, our forces must be able to operate even while under attack in cyberspace. The DoD

Cyber Strategy also directs U.S. cyber forces to target adversary weaknesses, offset adversary strengths, and enhance the effectiveness of the Joint Force. In order to succeed, our cyber forces must be well trained, properly equipped, and provided with the operational latitude and properly delegated authority to prepare the battlefield in advance of potential conflict.

Based on the guidance provided in the National Security Strategy, the National Defense Strategy, and the National Cyber Strategy, the DoD Cyber Strategy sets five clear defense objectives in cyberspace.

First, the Department must ensure that the Joint Force can achieve its mission in a highly contested cyber domain. The credibility of our military deterrence depends upon making clear that we are prepared to fight and win even against a capable modern adversary. Our systems must be cyber-hardened, resilient, and secure.

Second, cyber operations must enhance U.S. military advantages and strengthen the Joint Force. Cyber capabilities can increase the speed, reach, and precision of the Joint Force by creating novel, temporary, or reversible effects unmatched by traditional weapons. We are working to expand the scope and capacity of our cyber capabilities and to integrate them into Joint Force planning, exercises, and training.

Third, we must defend national critical infrastructure from significant foreign malicious cyber activity. This is a new area of emphasis for the Department and reflects the facts that competitors are targeting these assets, and that any large-scale disruption or degradation of national critical infrastructure, not just DoD infrastructure, would be a national security concern. We seek to preempt, defeat, or deter malicious cyber activity targeting national critical

infrastructure against a significant cyber incident by defending forward to stop threats before they reach their targets and will support the Department of Homeland Security in fulfilling its responsibility to coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure.

The fourth objective of the strategy is to secure sensitive DoD information wherever it resides. Nearly every day, the news features a report of a major hacking incident, and states like China are relentlessly seeking to acquire both classified and unclassified data that they can use to gain economic, political, or military advantage over the United States. Innovation is the seed stock of our future security, and the Department is taking a much stronger approach to protecting that information and the systems on which it resides.

Fifth and finally, the strategy prioritizes expanding cyber cooperation with our interagency, industry, and international partners to advance our mutual interests, including the protection of infrastructure upon which we rely.

The DoD Cyber Strategy also articulates a proactive and assertive approach for achieving these goals. It states that DoD cyberspace forces must be defending forward: disrupting threats at the source before they reach U.S. networks. This is an essential element of a defense-in-depth approach that protects the Nation from cyber threats, despite imperfect cybersecurity. The Department must routinely operate in non-U.S. networks in order to observe threats as they are forming and have the ability to disrupt them. This is also critical to increasing military readiness. We cannot be fully prepared to take effective action in a potential conflict unless we have already developed the tools, accesses, and experience via our actions day-to-day.

The necessity of this shift to a proactive approach was made clear in our efforts to secure the midterm elections by defending forward. USCYBERCOM and the National Security Agency (NSA) established an interagency group to fuse information, operational expertise, and resources to contribute to interagency efforts to protect the elections from foreign interference and influence. We expanded our cooperation with the Department of Homeland Security (DHS) and took steps to ensure that, if our assistance was requested, Defense Department personnel could provide support to DHS in a timely and effective manner. We also partnered with several European countries.

In addition to our immediate work to secure the 2018 U.S. midterm elections, the Department has taken further steps to translate our strategy into a plan of action. The first step was the completion of the first-ever Cyber Posture Review (CPR). The CPR involved a comprehensive analysis including data collection, war gaming, modeling, and extensive expert inputs from within and outside the Department. The CPR examined the resources, capabilities, manpower, and organization needed to implement the strategy, and identified existing gaps between where we are today and where we need to go to achieve our strategic objectives.

The CPR gap assessment drove the development of actionable lines of effort that are guiding the work of our cross-functional Principal Cyber Advisor Team. This team is growing to ensure it has the capacity to oversee the full range of actions needed to strengthen our cyber posture. This is a high priority for the Department. Mr. David Norquist, currently performing the duties of the Deputy Secretary of Defense, is personally overseeing bi-weekly meetings to ensure that we are holding leaders accountable for change. Although much work remains to

be done, we have made enormous progress in the past year and continue to build momentum.

Authorities and Policies

I would now like to provide some examples of specific changes we have been making to the way we operate in cyberspace. We have worked diligently, and in partnership with Congress, to ensure that the authorities and policies currently in place governing cyberspace operations enable our strategic approach to competing and prevailing in this domain. Several changes during 2018 have been particularly impactful. In the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA for FY 2019), the affirmation of the President's authority to counter active, systemic, and ongoing campaigns in cyberspace by our adversaries against the Government and the people of the United States (Section 1642) as well as the clarification that certain cyber operations and activities are traditional military activities (Section 1632) have been force multipliers. Thank you very much for your support. On the policy front, the President had approved updated policy on U.S. cyber operations.

These changes have advanced and modernized how the Department operates in cyberspace and enabled the missions described in the DoD Cyber Strategy. We have also worked hard to align our internal policies with our cyberspace objectives. In particular, we focused on how our cyber forces operate in the homeland. Last May, we reissued our memorandum on Defense Support to Cyber Incident Response (DSCIR). The DSCIR memorandum provides guidance to the Department on how DoD cyber capabilities can be employed in response to a request for support to augment civil authorities. We faced a real-world example of

this as we prepared for the 2018 U.S. midterm elections, when we worked to ensure that the appropriate procedures were in place in case we received a DSCIR request from DHS. Fortunately, DHS never had to make such a request. However, the lessons we learned during that period will be useful moving forward. My goal in the long-term is to normalize cyber support to civil authorities by fully integrating it into the Department's existing and long-standing policies and procedures for Defense Support to Civil Authorities (DSCA) across all domains.

Partnerships

In addition to updating our DSCA policies, we are continuing to refine Department guidance concerning the day-to-day partnerships between military cyber forces and State and local governments. We are currently reissuing a memorandum that provides policy guidance for all DoD personnel on the provision of cyber support and services to non-DoD organizations and activities when those services are provided incidental to military training. The memorandum also details how National Guard personnel can use certain DoD information, networks, software, and hardware for State cyberspace activities.

The DoD Cyber Strategy emphasizes the importance of working with partners to maximize our successes in this domain. To that end, we have devoted focused attention during the last year to building and enhancing our relationships with other U.S. Government departments and agencies, industry, and our allies and partners. Last year, Secretary Mattis and Secretary Nielsen signed a joint memorandum of understanding (MOU) detailing how our two departments can cooperate in order to secure and defend the homeland from cyber threats. The MOU reiterates DHS's primary role as the U.S. Government lead for protection of national critical infrastructure, and emphasizes DoD's unique mission of defending

forward. These roles are mutually reinforcing; DHS's efforts at home enable DoD to project power both in cyberspace and in the physical domains, even as our efforts outside the homeland help to secure U.S. infrastructure.

As part of the efforts to implement this MOU fully, DoD and DHS senior leaders, including myself, recently signed a charter creating a Cyber Protection and Defense Steering Group. This steering group provides us with visibility into existing areas of DoD-DHS cyber cooperation, enabling us to synchronize our efforts more effectively. By bringing leaders from both departments into the same working group, we are able to collaborate better, and to ensure that our two departments are able to address cyber threats synergistically, rather than work at cross-purposes.

One area of major concern for us is the theft of sensitive DoD information from our DIB partners. The scale and scope of this theft from the DIB are putting our future military technological advantage at risk. DoD continues to work with industry, in coordination with DHS, to implement cybersecurity protections and to share cyber threat information with DIB partners. We are taking a variety of actions to secure our information more effectively, including the formation of an interagency working group, led by the Federal Bureau of Investigation (FBI), to ensure that the U.S. Government is operating in a unified manner and maximizing the unique capabilities and authorities of every participating department or agency.

Our efforts to enhance our partnerships are worldwide. The Department will work to strengthen the capacity of our international allies and partners to increase DoD's ability to leverage its partners' unique skills, resources, capabilities, and perspectives to enhance our mutual cybersecurity posture. We are dependent on other countries for many services that enable the U.S. military to function,

including our communications networks and the physical infrastructure that enable power projection. To help ensure that our allies and partners are as robust as we need them to be, we are working to enhance the Department's cyberspace partner capacity-building capabilities by promoting standards for cybersecurity practices, building international situational awareness and information-sharing mechanisms, and broadening DoD's coalition of close cyberspace partners.

We are also pressing our global partners to hold states that are acting irresponsibly in cyberspace accountable for their actions. At our bilateral and multilateral engagements, we advocate responsible state behavior in cyberspace during peacetime. We know that some of our competitors act irresponsibly in pursuit of their national interests. Consequently, we are working with other countries to enhance our combined ability to impose consequences in response to malicious and destabilizing behavior in cyberspace.

A third international issue that we have prioritized is advocating for secure telecommunications networks and supply chains. We are engaging with our allies and partners to encourage them to maintain secure and reliable networks and information technology supply chains, including as it applies to their 5G telecommunications infrastructure. This is especially critical for countries with whom we have strong defense relationships. Our military relies on secure and resilient telecommunications infrastructure to operate alongside foreign forces. These risks can persist even outside the borders of those countries as a result of equipment exports and service contracts. We routinely encourage allies and partners to consider the risks they are building into their networks and supply chains when awarding contracts, and we urge them to exercise vigilance to ensure their security is guaranteed.

Cybersecurity and Personnel Reform

The CPR made it clear that the Department will not be able to achieve its objectives in cyberspace by continuing to conduct "business as usual." When it came to cybersecurity, it was clear that we needed to prioritize more effectively how we were spending money, allocating resources, and recruiting and retaining the most qualified people.

Our PCA team worked with the DoD Chief Information Officer (CIO) to identify the "Top Ten" areas where we faced the greatest risk. We prioritized these Top Ten areas during our most recent budget cycle and are currently working through pilot programs to implement solutions for several of them.

One focus area from the Top Ten is enhancing the recruitment and retention of the cyber workforce. In 2015 (FY 2016), Congress gave the Department the authority to create the new DoD-Cyber Excepted Service (CES) personnel system. The CES allows for the more agile recruitment of candidates with cyber expertise by streamlining HR procedures and delivering more competitive market-based salary packages. To date, 403 civilian positions have been converted from the competitive service to the CES positions across U.S. Cyber Command, Joint Force Headquarters DoD Information Networks, and the DCIO Cybersecurity Directorate. Currently, we are in the process of completing phase II CES implementation across the Service Cyber Components and the Defense Information Systems Agency (DISA), which spans approximately 15,000 positions. The CES is a key initiative within the "First Four," a subset of the Top Ten. We are focused on driving the pace of the CES to ensure we recruit, retain, develop, and train the best cyber professionals to execute the Department's mission

successfully. The Department continues to address the new hiring authorities (pay enhancements, direct hiring authority, and targeted local market supplements) to address the implementation requirements outlined in the Cyber Strategy. To that end, we are working closely with the Office of the Under Secretary of Defense for Intelligence (USD(I)) to improve the security clearance process to ensure that when we attract the best talent we are also able to onboard those individuals in a timely manner. We are also energizing the uniformed services to use their recently-granted authorities to recruit and retain the best and brightest military officers with deep cyber expertise..

Another new Department initiative is the Protecting Critical Technology Task Force (PCTTF), established last year at the direction of Secretary Mattis to improve protection of DoD technology. As Major General Murphy briefed this subcommittee last week, the PCTTF is integrating and accelerating the disparate DoD technology protection activities occurring across the Department and developing new innovative solutions for currently unaddressed problems. Cyber is, of course, a central concern of the PCTTF, and the Task Force is evaluating a range of measures to increase the cybersecurity and resilience of our DIB private sector partners.

Conclusion

In summary, our new strategy has provided us with a roadmap for achieving our objectives in cyberspace. We are now focusing on implementing that strategy and ensuring that the various elements necessary for success are properly aligned. We have made great strides in the last year. We have expanded authorities that enable our mission to defend forward. We are working to ensure that our internal policies support our vision for the Department's role in the homeland. And, we are

doubling down on collaborating with other departments and agencies, industry, and our international partners and allies. Notwithstanding the significant progress made, we understand there is still more work to be done. I look forward to working with you and our critical stakeholders, both within and outside the U.S. Government, to ensure that the U.S. military will continue to compete, deter, and win in cyberspace.