STATEMENT OF

MR. KENNETH RAPUANO

ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE

AND GLOBAL SECURITY

TESTIMONY BEFORE THE HOUSE ARMED SERVICES

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

AND THE HOUSE HOMELAND SECURITY SUBCOMMITTEE ON

CYBERSECURITY AND INFRASTRUCTURE PROTECTION

NOVEMBER 14, 2018

## INTRODUCTION

Chairwoman Stefanik, Chairman Ratcliffe, Ranking Members Langevin and Richmond, and members of the committees, thank you for the opportunity to testify on interagency cyber cooperation between the Department of Defense (DoD) and the Department of Homeland Security (DHS). Last week's mid-term elections serve as a timely inflection point to review the close collaboration between our two Departments, and I appreciate the opportunity to discuss the sea change in our partnership. I would like first to thank Congress for its broad and continued support of the Department's cyber missions, including the enactment of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which supports a range of military operations in cyberspace to disrupt, defeat, and deter malicious cyber activities.

## THE THREAT

Before reviewing the Department's strategic posture for cyberspace, I would like to offer a few observations on the threat environment. As the National Defense Strategy and 2018 DoD Cyber Strategy make clear, the homeland is no longer a sanctuary from cyber threats. The United States' strategic competitors are conducting cyber-enabled campaigns to erode U.S. military advantages, threaten our infrastructure, and reduce our economic prosperity. In particular, we are engaged in a long-term competition with China and Russia. These states have expanded that competition to include persistent campaigns in and through cyberspace that are individually below the threshold of armed conflict, but that collectively pose long-term strategic risk to the Nation, as well as to our allies and partners. Our strategic posture acknowledges the growing risk to our military advantage

and to the Nation if we do not deter, disrupt, and defeat these threats.

**STRATEGIC POSTURE**

In September, the President released the new National Cyber Strategy, which highlights the growing threat that malicious cyber actors pose to our national security. The 2018 DoD Cyber Strategy commits the Department to fulfill its role in the National Cyber Strategy. Nested within the National Security and National Defense Strategies, and released shortly after the release of the 2018 DHS Cybersecurity Strategy, the DoD Cyber Strategy prioritizes the challenge of Great Power competition and recognizes that the Department must adopt a forward-leaning posture to compete with, and counter, determined and rapidly maturing adversaries. It normalizes the cyberspace domain, integrating cyberspace operations into military operations in the physical domains of air, land, sea, and space. It also makes clear that DoD's focus in cyberspace, like in other domains, is to "defend forward"—that is, to prevent or mitigate threats before they reach U.S. soil. This focus complements the DHS Cybersecurity Strategy's emphasis on domestic preparedness and risk management. Together, the DoD and DHS strategies form a national, mutually supporting approach to "defense in depth."

Specific to our collaboration with DHS, the 2018 DoD Cyber Strategy identifies three important roles for DoD in defending the homeland. First, by defending forward, DoD will seek to preempt, defeat, or deter malicious cyber activity targeting the United States that could cause a significant impact. This includes malicious cyber activity that falls below the use of force.

Second, DoD will strengthen the resilience of networks and systems that

contribute to current and future U.S. military advantages. Past strategies have taken a narrow view of what the Department must defend to ensure it is capable of performing its assigned missions. The evolving cyber threat and increasingly provocative activities of key competitors have demonstrated threats and vulnerabilities that extend beyond the DoD Information Network, and this threat must be addressed as a priority. Our interagency, international, and private sector partners will be key to implementing this pillar of the strategy to ensure that DoD can operate in a contested cyber environment.

Third, DoD has prioritized partnerships. DoD will identify the means by which to support its partners, but it also will seek to identify ways those partners can inform and enable DoD missions. For example, DoD will leverage its intelligence and operational capabilities to provide indications and warning of malicious cyber activity to other Federal partners and the private sector. But, for these partnerships to be effective, information and threat intelligence must flow back to DoD to inform the conduct of cyber operations. Timely feedback between our organizations will continuously improve the quality of the information exchange.

We are moving aggressively to implement the DoD Cyber Strategy. As directed by the National Defense Authorization Act for Fiscal Year 2018, the Department conducted a comprehensive review of its cyber posture and ability to execute the Strategy. The review included extensive background research, data collection, and expert interviews. This classified review identified that we must continue investments in our people, capabilities, and processes to meet fully the objectives set forth in the Strategy. Secretary Mattis and Deputy Secretary Shanahan are directly engaged in these efforts, and we have already identified, prioritized, and assigned leads to begin

implementing the Strategy across nine lines of effort.

**TRANSLATING STRATEGY TO ACTION**

With these new strategies in place, we have the right policy and guidance to support the defense of the United States in cyberspace. In response, DoD and DHS have worked together to establish a framework to drive domestic preparedness and critical infrastructure efforts. The 2018 mid-term elections are the first test of this expanded cooperation.

Secretary Mattis and Secretary Nielsen recently signed a joint memorandum that frames how DHS and DoD will secure and defend the homeland from cyber threats. This is a major step in fostering closer cooperation and marks a sea change in the level of collaboration between our Departments. The memorandum makes clear that DHS's mission to protect critical infrastructure and DoD's mission to defend the homeland by defending forward are mutually reinforcing. DoD and DHS each derive unique insights from our daily activities—whether from DoD's intelligence collection and cyber operations, or from DHS's cyber operations to protect federal networks and critical infrastructure in partnership with the private sector—that inform our respective missions.

Implementation of the joint memorandum is already underway. Yesterday, I joined my DHS and Joint Staff colleagues to sign the Joint DoD-DHS Cyber Protection and Defense Steering Group Charter. Established at the direction of Secretaries Mattis and Nielsen, this Steering Group will apply senior leadership energy to enhance U.S. Government readiness against cyber threats.

In this vein, DoD and DHS cooperated to ensure that all appropriate Federal government tools and resources were available to protect and defend the 2018 mid-term elections from foreign interference. As part of this effort, DoD provided standing approval for DoD personnel to support DHS cyber incident response activities in the event of a significant cyber incident impacting elections infrastructure that would have required a request for assistance from DHS. In preparation for a request for assistance from DHS, DoD dispatched an advance team to DHS's National Cybersecurity and Communications Integration Center to improve situational awareness, communication, and team integration for better unity of effort should DHS request assistance from DOD.

The National Guard also played an important role in election support. Governors from several States used National Guard personnel in State status to support election cybersecurity in accordance with State law and policy. Examples of support included training exercises with local and State cyber officials and critical infrastructure partners, vulnerability and risk assessments, and information sharing. In addition, DoD authorized National Guard personnel in State active duty status, who already have security clearances, to access Top Secret Sensitive Compartmented Information to support securing the elections more effectively.

**PATHFINDERS AND PLANS**

Beyond elections, DoD is focused on how to improve collaboration with DHS in support of DHS's mission to assist the private sector with protecting critical infrastructure. Through a series of pathfinder initiatives, we are supporting DHS's efforts to enable

private sector entities to defend their networks by sharing relevant threat information. In turn, these pathfinders will enable DoD to partner with DHS in order to leverage private sector threat information to inform DoD cyberspace operations. We've begun our initial pathfinder effort through DHS with the financial sector and are working with DHS to establish a second pathfinder with the energy sector to build upon our existing information sharing efforts with the Department of Energy (DOE).

Separately, we are strengthening the Defense Industrial Base (DIB) Sector partnership to improve the security and resilience of DIB critical infrastructure. Specific lines of effort include: advancing information sharing, assessing and reforming DoD's approach to identification and risk management of DIB critical assets, and shielding future critical assets while they are still in development. This approach aligns with the National Defense Strategy guidance to enhance Joint Force lethality and reform Departmental procedures, and it complements our strategic approach on improving cybersecurity.

DoD is also coordinating with DHS's National Policy and Programs Division to establish a joint plan for future cyber incident response that required a request for assistance from DHS. At the tactical level, this effort has yielded a draft concept of operations that articulates how DoD's Cyber Mission Forces (CMF) would operate in support of DHS's Hunt and Incident Response Teams (HIRTs) in the event of a significant cyber incident. By identifying roles, responsibilities, and coordination mechanisms, we are jointly establishing a baseline for smooth, efficient, and effective interagency operations.

Lastly, I would be remiss if I didn't highlight the National Guard's contribution to

DoD and the Nation. The National Guard and Reserve are fully integrated into the CMF and will continue to grow. As a component of the total force, we continue to assess how best to leverage the unique position, relationships, and skill sets within the National Guard. We fully recognize the National Guard's two complementary roles as an integral part of the total force and as a State capability. Section 1653 of the National Defense Authorization Act for Fiscal Year 2019, which requires an assessment of the feasibility and advisability of establishing Cyber Civil Support Teams, provides an opportunity to review and refine the role of the National Guard. My team will lead this review with the Department of Homeland Security.

**CONCLUSION**

Thank you again for the opportunity to appear before you today. As you can see, the Department has undertaken extensive work with DHS to improve defense of the homeland and critical infrastructure, but there is much left to do. I look forward to working with Congress as we address these challenges facing the homeland, and I welcome your questions.