STATEMENT OF

MR. KENNETH RAPUANO

ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE & GLOBAL SECURITY

TESTIMONY BEFORE THE

SENATE ARMED SERVICES COMMITTEE

OCTOBER 19, 2017

Thank you Chairman McCain, Ranking Member Reed, and Members of the Committee. It is an honor to appear before you to discuss the roles and responsibilities for defending the Nation from cyberattacks of significant consequence. I appear before you today in my role 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 DoD's strategy, policy, and strategic guidance to achieve DoD's cyber missions, goals, and objectives; lead the Department's interagency cyber coordination efforts, including for cyber incident response; advise the Secretary and the Deputy Secretary on cyber-related activities that support or enable DoD's missions in and through cyberspace; and, perhaps most relevant to today's discussion, ensuring that cyber forces and capabilities are integrated across all of DoD's priority missions, including mission assurance and Defense Support of Civil Authorities.

I have been requested to discuss the Department's role as part of an interagency response to a cyberattack of significant consequence. I am grateful to testify alongside my interagency colleagues because adequately addressing these important challenges requires a whole-of-government approach, of which the Department of Defense and its developing capabilities in cyberspace are just one part.

This is a timely and important topic because the threats and level of malicious activity we face in cyberspace are real and growing. This diverse and persistent set of threats comes from state and non-state actors who probe and scan U.S. networks for vulnerabilities. The states we watch most closely in cyberspace include China, Iran, North Korea, and especially Russia.

To address these threats, the Department is developing cyber forces and capabilities to accomplish three primary missions in cyberspace: 1) to defend DoD networks, systems, and information to ensure that DoD can accomplish its core missions; 2) to defend the United States and its interests against malicious cyber activities and cyberattacks of significant consequence; and 3) to provide integrated cyber capabilities in support of operational and contingency plans. Although all of the missions are important, given your focus today, my intent is to speak primarily about DoD's efforts to defend the United States and its interests from cyberattacks of significant consequence and its efforts to provide Defense Support for Civil Authorities, as these define DoD's role within a whole-of-government framework.

The Cyber Mission Force (CMF) is the Department's principal capability to carry out DoD's cyber mission. Consisting of more than 6,000 Soldiers, Sailors, Airmen, Marines, and civilians, the CMF achieved initial operational capability (IOC) in October 2016 and is projected to reach full operational capacity (FOC) by the end of this new fiscal year. Today, nearly 80 percent of the CMF's 133 teams have reached FOC. In recent years, the Department has made significant investments in building the workforce and systems to develop the CMF, and it continues to do so consistent with the FY2018 budget request. In terms of readiness, as well as operational activities in support of the campaign to defeat the Islamic State in Iraq and Syria (ISIS), DoD is already seeing the results of those investments. U.S. Cyber Command's increased experience, expertise, and capability drove the President's decision this summer to elevate U.S. Cyber Command to a Unified Functional Combatant Command, consistent with Section 923 of the National Defense Authorization Act of for Fiscal Year 2017. Among other benefits, elevation of the command will strengthen command and control and consolidate responsibility for cyberspace operations under a single commander, reporting directly to the Secretary.

Although many elements of the CMF contribute to defending the Nation against malicious cyber activities and cyberattacks of significant consequence, the Cyber National Mission Force through its integrated operations plays a key role. This force combines the capabilities of National Mission Teams (NMTs) that pursue adversaries into red space; National Support Teams (NSTs) that provide additional capacity in analysis, linguists, reporting, capability development, and targeting; and national Cyber Protection Teams (CPTs) that hunt adversaries in friendly terrain. As the primary counter-cyber forces, the integration of NMTs, NSTs, and national CPTs enhances our ability to learn the tactics, techniques, and procedures of our adversaries to detect malicious cyber activity. These teams develop and, if directed, undertake operations to deter, delay, disrupt, and defeat an imminent or ongoing cyberattack or malicious cyber activity. The combined efforts of these teams give the CMF the capacity to operate on a global scale against the broad spectrum of adversaries and growing threats.

Additionally, DoD is developing significant cyber capability and capacity within the Reserve Components, including the National Guard. The Air National Guard is developing 12 Air National Guard Squadrons to provide two full-time CPTs through rotations and is also providing three additional squadrons to deliver a portion of an NMT to the CMF. The Army National Guard has established the first of 11 CPTs, which will be built out through 2022. The U.S. Army Reserve will follow by establishing 10 teams of its own between now and 2024. Likewise, the Air Force Reserve is contributing personnel to fill three CPTs. All of these teams benefit from strong relationships with State and local authorities. To further strengthen these relationships and support preparedness, National Guard units may coordinate with, train, advise, and assist governmental entities outside DoD when incidental to military training in accordance with Section 2012 of Title 10, U.S. Code.

From both a deterrence and response standpoint, CMF teams are central to the Department's approach to cyber operations and to support U.S. Government efforts to defend the Nation against a cyber incident of significant consequence. With a goal of ensuring U.S. military dominance in cyberspace, these teams support the Department's efforts to deny the adversary the ability to achieve its objectives and, when directed, to conduct military actions in and through cyberspace in response to an imminent, ongoing, or recent attack or malicious cyber activity. Although DoD's focus is on preparing for and defending against cyberattacks of significant consequence, the President may determine that a military response to malicious cyber activity below the threshold of significant consequence or an armed attack is necessary and appropriate.

DoD's role in cyberspace goes beyond adversary-focused operations and includes identifying and mitigating our own vulnerabilities. DoD recognizes its own reliance on cyber-enabled critical infrastructure to conduct its core missions. The Department therefore understands congressional concerns regarding current and future cyber vulnerabilities and congressional efforts to authorize vulnerability identification programs. In response, we are working with our foreign partners and allies and our U.S. domestic partners, including the Department of Homeland Security (DHS), to identify cyber vulnerabilities in our networks, computers, critical DoD infrastructure, and weapon systems. In addition to these external partnerships, the Department is leveraging its own mission assurance risk-management processes to identify, prioritize, and mitigate the most impactful vulnerabilities to the critical infrastructure that is fundamental to DoD's ability to project power and protect the U.S. homeland, our people, and our allies and partners.

One last important element of our mission to defend the Nation is the Department's role as the sector-specific agency for the Defense Industrial Base (DIB), one of the 16 identified critical

infrastructure sectors. Using voluntary and mandatory reporting requirements, the Department partners with DIB sector stakeholders to maintain a robust cybersecurity and information assurance program to protect sensitive defense information and protect DoD networks and systems.

DoD has made significant progress; however, there is more to do, and we are only one piece of the broader whole-of-government effort to protect U.S. national interests in and through cyberspace. The outward, threat focus of DoD's cyber capabilities complements the strengths of our interagency partners, as we strive to improve resilience should a cyberattack of significant consequence occur. As articulated in law and policy, during cyber incidents, DoD may directly support the DHS's lead for protecting, mitigating, and recovering from domestic cyber incidents or, as appropriate and authorized by law, the Department of Justice's (DOJ) lead in investigating, attributing, disrupting, and prosecuting cybercrimes. Under DoD's broader Defense Support of Civil Authorities mission, the Department works closely with these domestic partners as they carry out their aforementioned responsibilities so that DoD is prepared to provide support when it is needed and DoD is called upon to do so. DoD also regularly works closely with domestic partners through cyber fusion center integration, robust information sharing arrangements, liaison and detailee programs, development of national plans, exercises to strengthen our response, and interagency deliberations on malicious cyber activity.

The significant work of U.S. departments and agencies has resulted in a common understanding of our various roles, responsibilities, and authorities. That said, it is clear we have more work to do to resolve seam and gap issues among various departments and agencies. DoD has taken a number of steps to address these problems and to improve both our readiness and that of our interagency partners. For instance, we are continually refining policies and authorities to

improve the speed and flexibility to provide support, and we organize and participate in exercises, such as CYBER GUARD, with a range of interagency, State, and local partners to improve our ability to respond to cyberattacks on critical infrastructure.

Although DoD has built capacity and unique capabilities, for a number of reasons, I would caution against ending the current framework and against reassigning more responsibility for incident response to the Department of Defense. First, DoD's primary mission is to provide the military forces needed to deter war and to be prepared to defend the country should deterrence fail, which requires us to be prepared at all times to do so. DoD is the only department or agency charged with this mission, and success in this requires the Department's complete focus. In this case, any significant realignment of roles and responsibilities will have opportunity costs, including absorptive capacity to build mission capability in a new area, especially ones that could distract the Department from its core warfighting missions.

Second, the United States has a long normative and legal tradition limiting the role of the military in domestic affairs. This strict separation of the civilian and the military is one of the hallmarks of our democracy and was established to protect its institutions. Designating DoD as the lead for the domestic cyber mission risks upsetting this traditional civil-military balance.

Third, a primary civil reliance on DoD in the steady-state would result in increased demands that could not be met without significant changes in resource allocation. We would expect even greater demand in a conflict scenario, when there might be a natural tension in the need to preserve DoD mission capabilities and requests for support to civilian agencies. Even with such a change in resource allocation, the addition of a new mission would likely detract from the focus on and readiness for the warfighting mission.

Finally, putting DoD in a lead role for cyber incidents creates an exception to accepted domestic response practice in all other domains, which would disrupt our efforts to establish and maintain unity of effort. Civilian agencies have the lead responsibility for domestic emergency response efforts; this should not be different for cyber incidents. The Federal Government should maintain a common approach to all national emergencies, whether they are natural disasters or cyberattacks.

I have confidence that the President's Executive Order 13800 signed in May will address many of Congress's concerns by helping to identify and address the shortfalls in the present system. Through reports and other deliverables, the Executive Order specifically targets the areas of protecting critical infrastructure, strengthening the deterrence posture of the United States, and building international coalitions. As a result, the Federal Government—especially DHS and Sector Specific Agencies—is identifying current and prospective authorities and capabilities that it could use to support the cybersecurity efforts of critical infrastructure entities. DoD is contributing to these efforts and conducting its own review of how best to protect the Defense Industrial Base from cyber vulnerabilities. Through this process, we should have a better understanding of the key challenges facing the U.S. Government in this area and a way forward for addressing them.

Therefore, my vision and highest priority in cyber are to address the challenges that still face the Department in cyberspace and its role in the broader interagency response effort. Specifically, I am working to reinvigorate the role of the Principal Cyber Advisor; to clarify the Department's internal lines of accountability and authority in cyber; and to integrate and communicate more effectively DoD cyberspace strategy, plans, and train and equip functions in cyber. It is also time to revise our Cyber Strategy, update policy on such key cyber issued as

deterrence, and translate this and other guidance into capabilities, forces, and operations that will maintain our superiority in this domain. Meanwhile, the Department must ensure that several strategic initiatives it is undertaking in cyber come to fruition, including the elevation of U.S. Cyber Command to a unified combatant command, implementing the Cyber Executive Order, initiating the Cyber Excepted Service, and identifying and mitigating vulnerabilities in DoD's networks, systems, and platforms. I look forward to working with Congress on these efforts and welcome its feedback.

In conclusion, the Department of Defense is committed to defending the U.S. homeland and is prepared to defend the Nation from cyberattacks of significant consequence that may occur in or through cyberspace. It has undertaken comprehensive efforts, both unilaterally and in concert with interagency partners, allies, and the private sector to improve our Nation's cybersecurity posture and to ensure that DoD has the ability to operate in any environment at any time. Our relationship with Congress is absolutely critical to everything the Department is doing. 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.