STATEMENT OF

MR. B. EDWIN WILSON

DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR

CYBER POLICY

TESTIMONY BEFORE THE HOUSE ARMED SERVICES

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING

THREATS AND CAPABILITIES AND THE HOUSE OVERSIGHT

AND REFORM SUBCOMMITTEE ON NATIONAL SECURITY

SEPTEMBER 10, 2019

INTRODUCTION

Chairman Langevin, Chairman Lynch, Ranking Member Stefanik and Ranking Member Hice, and members of the committees, thank you for the opportunity to testify on the role of the Department of Defense (DoD), in partnership with other Federal departments and agencies, in securing the Nation's internet architecture.

I would first like 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 (NDAA) for Fiscal Year 2019, which supports a range of military operations in cyberspace to deter, disrupt, and defeat, malicious cyber activities, as well as our constructive, ongoing dialogue with the House and Senate Armed Services Committees regarding the development of the NDAA for Fiscal Year 2020.

THE THREAT

To begin, I would like to offer a perspective on the cyber threat environment. As the 2018 National Defense Strategy and the 2018 DoD Cyber Strategy make clear, the U.S. 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 Nation's critical infrastructure, and compete using predatory, non-free market economic practices to undermine our prosperity.

In particular, we are engaged in long-term power competition with China and Russia. As part of this long-term power competition, these States are engaged in persistent campaigns against the United States in and through cyberspace. These campaigns are conducted below the threshold of armed conflict but collectively pose long-term strategic

risk to the Nation, our allies, and our 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. The Department, working alongside our U.S. Government partners, continues to strengthen public and private partnerships in order to mitigate emerging cyber threats, but more must be done and will be done.

STRATEGIC POSTURE

In September 2018, the President released the National Cyber Strategy, which highlights the growing threat that malicious cyber actors pose to our national security. The 2018 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. The strategy normalizes the Department's efforts in the cyberspace domain, integrating cyberspace operations into military operations in the physical domains of air, land, sea, and space.

The DoD Cyber Strategy also makes clear that the Department's focus in cyberspace, like in other domains, is to "defend forward"—that is, to prevent or mitigate threats before they harm U.S. national interests. We defend forward by conducting operations that range from collecting information to gain insight about hostile cyber actors and their intent, to exposing malicious cyber activities and associated infrastructure publicly, to disrupting malicious cyber activities directly. Through a persistent day-to-day presence in cyberspace, we can best monitor our adversaries and develop an effective national cyber defense. This approach simultaneously imposes costs on adversary malicious actors and enables our interagency, industry, and international partners to strengthen their resilience, close

vulnerabilities, and defend critical networks and systems.

In parallel with defending forward, the Department is continually working with its partners to strengthen the resilience of networks and systems that contribute to current and future U.S. military advantages. The Department has previously focused its defensive efforts on military platforms and systems and networks owned and operated by DoD. However, the evolving cyber threat and increasingly provocative activities of key competitors have demonstrated vulnerabilities that extend beyond the DoD Information Network. The vulnerability of U.S. critical infrastructure to cyberattacks means that adversaries could disrupt military command and control, banking and financial operations, the transportation sector, the energy sector, and various means of communication. As a result, supporting U.S. Government efforts in securing and defending the Nation's critical infrastructure is also a priority under the DoD Cyber Strategy.

Our interagency, international, and private sector partners are key to ensuring that DoD can operate and project power in a contested cyber environment. Empowered by the 2018 DoD Cyber Strategy, DoD's role in defending the homeland is focused outward and supports our interagency partners, including the Department of Homeland Security (DHS), represented here this afternoon by Assistant Director Manfra. Supporting U.S. Government efforts to secure and defend U.S. critical infrastructure has become an enduring DoD activity, as demonstrated in the successful whole-of-government effort to secure the 2018 U.S. midterm elections.

CHALLENGES TO SECURING THE NATION'S INTERNET ARCHITECTURE

It has become increasingly clear, as the National Security Strategy released in December 2017 identified and as President Trump has noted, that "economic security is national security." A strong, defensible cyber infrastructure fosters economic growth, protects our liberties, and advances our national security. As the U.S. military becomes more and more technologically advanced, our demand for connectivity that's always-on and always available will only increase. DoD relies heavily upon the global internet architecture including internet exchange points, data centers, content delivery networks, undersea cables, international telecommunications, and related infrastructure. Undersea cable systems are vital to the execution of DoD's missions globally. The Department has been leasing bandwidth on privately-owned undersea cable systems since the 1980s. DoD prioritizes mission-essential traffic and the Defense Information Systems Agency (DISA) is constantly working with the Combatant Commands, Military Departments, and Defense Agencies to meet mission requirements.

The U.S. Government has a limited and specific role to play in defending against attacks on our Nation's internet architecture, including through DoD's trusted relationships with industry. Security was not a major consideration when the Internet was designed and fielded. Although computers and network technologies underpin U.S. military warfighting superiority by enabling the Joint Force to gain the information advantage, strike at long distance, and exercise global command and control, the private sector owns and operates well over ninety percent of all of the interdependent networks of information technology infrastructures across the cyber domain. At the same time, the Nation's telecommunications infrastructure is primarily owned by commercial entities. Our adversaries target our Nation's weakest links, and vulnerabilities are consistently found across the full scope of the

Internet ecosystem be it government or industry targets.

The Department, which views the challenges it faces in performance of its critical missions principally through a national security lens is nonetheless highly dependent on privately-owned infrastructure, decisions concerning which are regularly guided by ordinary business – or economic – considerations. Recognizing this inherent tension, defending national critical infrastructure, including the Nation's internet architecture, from significant foreign malicious cyber activity has become an area of increased emphasis for the Department.

Any large-scale disruption or degradation of national critical infrastructure would constitute a national security concern, as would threats to DoD critical technology information (CTI) and other controlled unclassified information (CUI) processed or stored on non-DoD-owned systems and networks, demanding close cooperation and strong relationships with the private sector. This priority is formalized in the DoD Cyber Strategy's directive that the Department be prepared to defend assertively non-DoD-owned Defense Critical Infrastructure – referring to the composite of DoD and non-DoD assets essential to develop, project, support, and sustain military forces and operations worldwide. Presidential Policy Directive-21, "Critical Infrastructure Security and Resilience," prescribes that DoD is the Sector Specific Agency (SSA) for the DIB critical infrastructure sector. As the Federal lead of the DIB critical infrastructure sector, DoD and DIB partners work together to improve security and resilience of DIB networks and systems, working closely with DHS and other partners.

The Department's cybersecurity initiatives are an important aspect of the overall and ongoing efforts to deny, disrupt, and neutralize critical technology transfer to China. In October 2018, the Secretary of Defense established the Protecting Critical Technology Task Force (PCTTF) to align the Department's efforts to protect its critical technologies and

address broader systematic issues. Through the work of this Task Force, the Department is driving protection efforts towards its most critical technologies, elevating security across our Research, Development, and Acquisition communities, and organizing the Department's operational response as warranted. In addition, under Executive Order 13873, Securing the Information and Communications Technology and Service Supply Chain, DoD will work with the Department of Commerce to limit foreign adversaries' ability to create and exploit vulnerabilities in our national information and communications technology in order to commit malicious cyber-enabled actions against US critical cyber infrastructure.

DoD is focused on how to improve collaboration with industry and other Federal departments and agencies, including DHS, the Federal lead for improving the security and resilience of much of the Nation's critical infrastructure and SSA for telecommunications. Our partnership with industry includes cyber threat information sharing and collaboration to better protect DoD information as well as industry intellectual property. It will take a whole-of-society partnership to defend our vital interests successfully in an era of intensifying adversarial competition.

COLLABORATING WITH INTERAGENCY AND INDUSTRY PARTNERS

In support of one of the Department's most critical interagency partnerships, DoD and DHS have worked together to establish a framework to drive domestic preparedness and critical infrastructure efforts. In October 2018, then-Secretary of Defense Mattis and then-Secretary of Homeland Security Nielsen signed a joint memorandum that frames how DHS and DoD will secure and defend the homeland from cyber threats. 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 underway. A Joint DoD-DHS Cyber Protection and Defense Steering Group Charter was signed in November 2018, and the Steering Group leadership has directed the prioritization of cyber security cooperation between our departments and meets regularly to assess our progress.

DoD and DHS worked together to ensure that all appropriate Federal Government tools and resources were available to protect and defend the 2018 U.S. midterm elections from foreign interference. As part of this effort, DoD regularly shared information with DHS and the Federal Bureau of Investigation (FBI). It also provided standing approval for DoD personnel to support DHS cyber incident response activities in the event of a significant cyber incident impacting elections infrastructure. 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 if DHS requested DoD assistance.

Beyond elections, the Department works closely with DHS, FBI, and stakeholders from across the Federal Government, the private sector, and international partners concerning risks to critical infrastructure, including telecommunications networks. Through a series of Pathfinder initiatives, DoD is focused on improving its collaboration with DHS and other SSAs in support of their missions to assist the private sector – including select critical infrastructure partners – by sharing threat information, conducting collaborative analysis of vulnerabilities and threats, and mitigating those risks.

Whole-of-nation collaboration is crucial to our ability to build resilience and deter or defeat strategic threats to U.S. national interests and infrastructure. Although the Department supports DHS's efforts to enable private sector entities to defend their networks, these Pathfinders in turn enable DoD to partner with DHS to leverage private sector threat information to inform DoD cyberspace operations.

CONCLUSION

Thank you again for the opportunity to appear before you today. With the 2018 National and DoD Cyber Strategies in place, the Department has the right policy and guidance to support the defense of our Nation in cyberspace. The Department has undertaken extensive work with DHS and other SSAs to improve our collective defense of the homeland and the Nation's internet architecture. That said, there is much left to do. I look forward to working with Congress as we address these challenges, and I welcome your questions.