STATEMENT BY

BRIGADIER GENERAL DENNIS A. CRALL
U.S. MARINE CORPS
SENIOR MILITARY ADVISOR FOR CYBER POLICY
DEPUTY PRINCIPAL CYBER ADVISOR

ON BEHALF OF THE DEPARTMENT OF DEFENSE

TESTIMONY BEFORE THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON
INTELLIGENCE, EMERGING THREATS, AND
CAPABILITIES

ON

"DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY, CYBERSECURITY, AND INFORMATION ASSURANCE"

FEBRUARY 26, 2019

NOT FOR PUBLICATION UNTIL
RELEASED BY THE HOUSE ARMED SERVICES COMMITTEE

Good afternoon Chairman Langevin, Ranking Member Stefanik, and Members of the Intelligence, Emerging Threats, and Capabilities Subcommittee. Thank you for the opportunity to testify before the Subcommittee regarding our combined partnership in achieving the Department's information technology (IT), cybersecurity, and information assurance efforts. I appear before you today in my roles as the Senior Military Advisor for Cyber Policy and the Deputy Principal Cyber Advisor to the Secretary of Defense.

As provided in Section 932 of the National Defense Authorization Act for Fiscal Year (FY) 2014, the Principal Cyber Advisor (PCA) serves as the civilian Department of Defense (DoD) official who acts as the principal advisor to the Secretary of Defense on the Department's military and civilian cyber forces and activities. The Office of the PCA (OPCA) synchronizes, coordinates, and oversees the implementation of the Department's Cyber Strategy and other relevant policy and planning documents to achieve DoD's cyber missions, goals, and objectives. At the core of the OPCA is the Cross Functional Team (CFT) of detailees from the Military Departments, Services, and Defense Agencies. The CFT provides an objective and broad perspective needed to ensure that outcomes match short- and long-term approved, strategic visions. To meet increasing demands outlined in the DoD Cyber Strategy Lines of Effort (LOE) and the DoD Cyber Posture Review's gap analysis, the Deputy Secretary of Defense has made a substantial investment in the OPCA, adding permanent billets including an OPCA Deputy for long-term continuity.

The OPCA executes the DoD Cyber Strategy, including by addressing the gaps identified in the DoD Cyber Posture Review, through the LOE implementation process. The LOE implementation process allows the Department to take a system-wide view of the environment, address disparate approaches, and eliminate friction points across the Department. Although the LOE end-states, articulated in the Cyber Strategy, are enduring, the intermediate objectives are more dynamic to allow the Department to re-evaluate and adjust as needed to the operating environment. OPCA activities are rooted in strategy and prioritized by risk; they are warfighter-focused with the aim of increasing the lethality of the U.S. Armed Forces. To that end, we are leading a Department-wide effort to translate the Cyber Strategy LOEs into specific objectives, tasks, and sub-tasks that are focused on outcomes. Integral to this effort is the ability to measure results clearly and objectively to be able to gauge return on investment.

The DoD's "Top 10 Cyber Priorities" are nested under the Cyber Strategy LOEs to ensure consistency and completeness of execution. Through implementing the "First Four (a sub-set of the Top 10)," the OPCA is focused on outcomes to improve end-point security, identification and access management, development security operations, and cyber workforce management. The FY 2019 objectives are aggressive and include end-point detection and automated reporting of devices with an operating system; the development and deployment of a DoD Enterprise Identity Service; establishment of a developer's toolkit; and roll-out of Cyber Excepted Service Phase II. A DoD re-programming request is pending to enable these mission critical activities.

Together, the DoD Chief Information Officer (CIO) and the OPCA work together directly to implement the DoD Cyber Strategy in close coordination with the other DoD Component CIOs. The DoD CIO and PCA co-lead weekly meetings focused on cyber issues with the Deputy Secretary of Defense and with all of the Military Departments' and Office of the Secretary of Defense (OSD) Principals present. These meetings ensure that the Deputy Secretary of Defense is kept abreast of progress on cyber initiatives and that all Department leaders are present to receive direction, share challenges, leverage opportunities--all with the purpose of achieving timely and measurable outcomes.

The Department has an ongoing commitment to information technology, cybersecurity, and information assurance as articulated in our Cyber Strategy. To that end, I will continue to partner across the Department as an advocate to integrate and oversee the development of cyberspace capabilities, activities, and policies, within cyber-related initiatives. The OPCA with its cross-functional team has proven to be a valuable component in translating plans to actions. Partnerships with the DoD CIO, the Military Departments, the Services, and other DoD Components could not be stronger and are key to continued success.

I am grateful for Congress's strong support of the Department of Defense's efforts to build the correct partnerships needed to operate in cyberspace to increase the lethality of our Armed forces. I thank the Subcommittee for its interest in these issues and look forward to your questions.