STATEMENT OF

VICE ADMIRAL MARSHALL LYTLE

DIRECTOR COMMAND, CONTROL, COMMUNICATIONS

AND COMPUTERS/CYBER, JOINT STAFF

BEFORE THE SENATE ARMED SERVICES

SUBCOMMITTEE ON CYBERSECURITY

MAY 23, 2017

INTRODUCTION

Chairman Rounds, Ranking Member Nelson, and Members of the Subcommittee, thank you for inviting us to discuss the Joint Force's efforts in cyberspace. I appreciate the opportunity to explain the progress made to improve America's cyber defense posture.

I will focus my comments on three primary missions in cyberspace and describe the current approach to strengthening the cyber warfighting capabilities of the Joint Force. Toward that end, I will describe the state of our ongoing efforts to man, train, and equip the Cyber Mission Force, as well as the Joint organizations needed to Command and Control them. Finally, while I cannot discuss particulars in an unclassified statement, I will broadly describe the cyber capabilities needed to support both offensive and defensive teams.

JOINT STAFF ROLE

As part of my duties as the Director for Command, Control, Communications and Computers/Cyber, I work with our Joint Staff Operations, Planning and Resourcing leaders to integrate strategic cyberspace matters, including synchronization with national strategies, readiness tracking of joint cyber forces, and development of capabilities and concepts to support the Chairman's decision making. We work closely with the Principal Cyber Advisor, the Office of the Secretary of Defense staff and the Services to assess, address and advocate for the Combatant Commands' cyber mission requirements and priorities in support of the National Defense Strategy.

PRIMARY MISSIONS IN CYBERSPACE

The Joint Force executes the Defense Department's three primary cyber missions in support of the National Defense Strategy. The Joint Force defends the Department's networks, systems, and information. The United States military's dependence on cyberspace for operations led the Secretary of Defense

in 2011 to declare cyberspace an operational domain for purposes of organizing, training, and equipping United States military forces. The Joint Force must be able to secure networks against attack and recover quickly if security measures fail. To this end, network defense operations are conducted on an ongoing basis to securely operate the Department of Defense Information Networks. When indications of hostile activity are detected within networks, the Joint Force has capabilities to react, recover and return the networks and systems to a secure posture. Accordingly, network defense operations on Department's networks constitute the vast majority of the Joint Force's efforts in cyberspace.

In addition to protecting Defense Department networks, the Joint Force must be prepared to defend the United States and its interests against cyberattacks of significant consequence when directed by the President or his national security team. This second cyber mission is performed on a case-by-case for significant cyber events that may include loss of life, significant damage to property, serious adverse United States foreign policy consequences, or serious economic impact on the United States.

Third, when directed by the President or the Secretary of Defense, the Joint Force must provide integrated cyber capabilities to support military operations and contingency plans. Examples include cyber operations that disrupt and adversary's military related networks or infrastructure in order to terminate an ongoing conflict on United States terms, or to disrupt an adversary's military systems to prevent the use of force against United States interests. United States Cyber Command, in coordination with other United States Government agencies, may be directed to conduct cyber operations to deter or defeat strategic threats in other domains. These primary missions are underpinned by three main cyberspace capability elements used to assess Combatant Commands' ability to execute their operational plans.

ELEMENTS OF CYBERSPACE CAPABILITY

This statement will not include information about offensive force or capability due to its classification, however, offensive components are important and are coupled with our defensive forces and capabilities to achieve maximum effects.

Cyber forces, cyber defenses and defensible cyber terrain are the three main elements that determine the Joint Force's our ability to achieve the primary cyber missions. Together, these elements factor into our ability to prevail against determined and capable nation-state cyber threat actors.

Of the cyber forces, the first line of defense -- "fixed force defenders" -- that operate and defend assigned network enclaves and associated defenses. Sometimes referred to as "cyber enterprise defense forces", they are composed of military cyber units that form the backbone of secure network operations. They include Service and Agency Network Operations and Security Centers, Cyber Security Service Providers, and Cyber Incident Response Teams, among others.

The Cyber Mission Force (CMF) is the Joint Force's "maneuver force" in cyberspace. The CMF is composed of 133 teams with objectives that directly align to the Department's three cyber missions. These tactical teams are command and controlled by a planning and execution structure led by United States Cyber Command through its subordinate Joint Force Headquarters.

The second capability element, dedicated cyber defenses, are arrayed in a defense-in-depth posture with a focused level of tiered defenses including the Department's Internet Access Point defense suites, the Joint Regional Security Stacks, and Service and Agency network security boundaries at the organizational and installation levels. These tiered defenses comprise our primary defense against external threats in cyberspace.

The final main element of the Department's cyberspace capabilities is defensible cyber terrain. The nature of cyberspace means that individual end-user machines are directly susceptible to compromise, and that a single compromise can quickly proliferate laterally to other machines. This inside threat coupled with the human factor introduced by users necessitates the protection of all networked systems to a specified minimum level of cybersecurity. Over the past year, the Department made significant gains in hardening our systems under the Department Cybersecurity Scorecard effort. Coupled with increased end point security, we must continue to train all personnel until they have a working knowledge of cybersecurity practices, and hold leaders accountable for instilling a culture of cybersecurity discipline.

Further improving the defensibility of cyber terrain involves systematically identifying "Mission Relevant Cyberspace Terrain" and obtaining situational awareness of that terrain in support of critical missions. Executing the DoD Cyber Strategy line of effort on mission assurance, the Joint Staff led a Department-wide initiative to bring together expert planners from the cyber defense and mission assurance communities to forge and codify a new approach to identifying the key cyber terrain that underpins the Joint Force's critical missions. This approach was vetted and refined during exercises. A formal Planning Order was sent out to all Combatant Commands last month toward that end, the culmination of 18 months of effort.

As the senior Joint Staff cyber leader, my main focus is on the manning, training and equipping of the cyber force. The remainder of my statement will focus on the successes and unique challenges faced in building and maintaining the world's premiere cyber force.

CYBER FORCES

The Joint Force's ability to man the cyber force is predicated on the

assumption that the force is a net exporter of cyber talent. Much like pilots, air traffic controllers and other highly technical military specialties, the Joint Force does not compete with industry, but rather is focused on building training programs and strategies to grow talent, leverage Reserve Component expertise, and retain adequate numbers of seasoned cyber operators to meet the growing demands in cyberspace. By anchoring our personnel strategies in net production vice competition, in addition to leveraging direct hires and native talent, we will be better able to produce adequate numbers of cyber experts while enhancing the collective cyber defense posture of our Nation.

Developing a training program for cyber operators resembles the challenge faced in training pilots and aircrew to operate the world's most advanced aircraft, maintaining their skills on the latest aircraft systems, and sustaining their numbers to ensure a constant sufficiency of motivated and technically excellent personnel. Creating a "pipeline" in the United States military's air components took many years. I am unsurprised by the challenges encountered while constructing the training and personnel pipeline for the Cyber Mission Force.

The Joint Force completed the Cyber Mission Force Training Transition Plan in January of this year. The plan introduced a joint training model and addresses the Cyber Mission Force Reserve Component training demand. As part of this effort a training funding shortfall was identified, and the Joint Staff is working with the Office of the Secretary of Defense to mitigate this shortfall.

The make-up of the cyber force is unique in warfighting because one-third of its composition is civilian. This poses a unique recruiting and retention challenge. We appreciate the committee's focus on this unique challenge and Congress' efforts to improve our ability to address this issue with Section 1107 of the FY16 National Defense Authorization Act. The Department of Defense Chief Information Officer's office is pursuing a permanent fix via the implementation of

the Department's Cyber Excepted Service program.

Equally important to manning and training the Cyber Mission Force is evolving from the narrowly focused Service platforms employed by cyber operators to a standardized joint capability that equips the force effectively and efficiently with integration into existing planning and force development constructs. The framework for equipping the Cyber Mission Force for both defensive and offensive missions is built upon a family of interoperable systems from which the Cyber Mission Force can operate and synchronize operations. The Joint Force is conducting an Analysis of Alternatives to determine how best to equip the Cyber Mission Force with Title 10 mission platforms.

The Cyber Mission Force – all 133 teams -- met their Initial Operating Capability milestone in Oct 2016. All teams are also on track to meet their Full Operating Capability milestone by Oct 2018. More than half of the teams have already met their Full Operating Capability milestone and all 133 teams are actively performing their assigned missions defending DOD networks, protecting weapons platforms, and defending critical infrastructure. Despite these successes, there are still significant readiness challenges that impact the cyber force. Joint training standards have been published and instituted standardized readiness reporting in the Defense Readiness Reporting System in order to track and address these challenges. This nascent tracking capability is beginning to identify trends that will help us better shape Service policy and resourcing requirements in the future.

Each Service is working their unique cyber manpower challenges as part of their man, train and equip responsibilities. They have learned and adapted over the past four years, instituting a number of personnel policy changes to ensure the success of the Cyber Mission Force and its associated cyber tactical headquarters. For example, all of the Services are leveraging their Reserve

Components to augment Cyber Mission Force teams, either in whole or in part, while adding Federal, State and local cyber surge capacity allowing the nation to collectively respond to major threat activity in cyber.

The Navy and Marine Corps continue to utilize individual augmentees to fill gaps in their active duty Cyber Mission Force teams and are looking at other ways to utilize their Reserve Components to address critical skillsets and shortages. Also, the Air Force utilizes its reserve component to present 3 full teams to the Cyber Mission Force as part of their total force contribution. Behind these 3 “full-time equivalent” teams are 15 rotating reserve teams comprised of Air Force Reserve and Air National Guard members that provide 12 teams of surge capacity in addition to the 3 full time teams required by United States Cyber Command. Finally, the Army Reserve Component began building an additional 21 teams to augment the original 133 Cyber Mission Force teams as well. Once fully built, the reserve Component will be providing approximately a fifth of the total Cyber Mission Force surge capacity of 166 teams. The build and training plan for these additional Reserve Component forces is included in the Cyber Mission Force Training Transition Plan referenced earlier should you wish further details.

The Cyber Mission Force continues to grow and mature, as does the increasing need to Command and Control and synchronize the global efforts of this complex and geographically dispersed warfighting capability. The Joint Staff recently completed a revised Command and Control model that streamlines the command relationships and synchronizes actions in support of Combatant Command campaigns. This model, coupled with manpower assessments performed by a team of joint manpower experts last summer and fall, informed a Joint Manpower Validation effort completed last month. The Department is currently working with the Services to review resourcing requirements for the

future.

CONCLUSION

Thank you again, Mr. Chairman, Ranking Member Nelson, and Members of the Committee for the opportunity to provide this statement. I am grateful for the Committee's oversight and your support for our men and woman in uniform.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu