STATEMENT BY

MAJOR GENERAL LORI E. REYNOLDS

COMMANDER

MARINE CORPS FORCES CYBERSPACE COMMAND

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY

CYBER POSTURE

March 13, 2018

Major General Loretta E. Reynolds
Commander, Marine Forces Cyber Command

Major General Reynolds was commissioned a Second Lieutenant in May 1986 upon graduating from the United States Naval Academy. Throughout her career she has served in a variety of command and staff billets in the operating forces. As a Lieutenant, she served as a Communications Watch Officer at the Base Communication Center, and later returned to the Division Communications Company where she served as a Communication Center Platoon Commander, Multichannel Platoon Commander, Operations Officer, and Radio Officer. As a Captain and Major, she served with Marine Wing Communications Squadron 18, 1st Marine Aircraft Wing Okinawa, Japan as a Detachment Alpha Executive Officer and Commanding Officer. She served with the Ninth Communication Battalion, 1st Surveillance, Reconnaissance, and Intelligence Group as the Assistant Operations Officer and Commanding Officer, Bravo Company. As a Lieutenant Colonel, she commanded Ninth Communication Battalion, I MEF and deployed in support of Operation Iraqi Freedom II in Fallujah, Iraq. As a Colonel, she commanded I MEF Headquarters Group and deployed the Group to Camp Leatherneck, Afghanistan in support of I MEF FWD/Regional Command Southwest in Helmand Province during Operation Enduring Freedom. She recently served as the Commanding General, Marine Corps Recruit Depot/Eastern Recruiting Region, Parris Island, SC.

In the Supporting Establishment, she has served as an Acquisition Project Officer at the Marine Corps Systems Command, Candidate Platoon Commander for Charlie Company, Officer Candidate School, Commanding Officer of Recruiting Station Harrisburg, Pennsylvania, an Action Officer and Deputy Division Head for Strategic Plans Division, Command, Control, Communications, and Computers (C4) Department, Headquarters Marine Corps and as Division Chief (J6) at the Joint Staff in the Pentagon. Her most recent assignment was as the Principal Director (Asia & Pacific), Office of the Deputy Under Secretary of Defense (Asia & Pacific).

Her professional military education includes the United States Naval Academy, The Basic School, the Basic Communication Officer's Course, Command and Control Systems Course, the Navy War College and the Army War College. She has earned Masters Degrees from both the Naval War College and the Army War College.

Her personal decorations include the Defense Superior Service Medal, Legion of Merit, Bronze Star, Meritorious Service Medal (with gold star), the Navy and Marine Corps Commendation Medal (with gold star).

Introduction

Chairman Rounds, Ranking Member Nelson, and distinguished members of this Committee, I thank you for inviting me here today to represent the Marines and civilian Marines of Marine Corps Forces Cyberspace Command (MARFORCYBER). I appreciate this opportunity to update you on the tremendous progress we have made since I was last before this committee in May, to highlight what your Marines are doing in the cyberspace domain and how we have shifted our focus from building the command to operationalizing, sustaining, and expanding capabilities in this warfighting domain.

Our Commandant, General Neller, made clear in his Message to the Force 2018 that the Marine Corps must be prepared to fight in order to make it to the next conflict. This includes our ability to fight – and win – in the domain of cyberspace. Our adversaries will test our superiority across the domains of air, land, sea, and space, in the next conflict. They are testing us in cyberspace today. Understanding this, and consistent with our Commandant's guidance, we are developing the Marine Corps' cyber capacity at the tactical level of war, so that in the future the Marine Corps will more effectively preserve the ability to fight and win in a contested environment and deliver effects in cyberspace.

It gives me great pride to share with you today the many accomplishments of the Marines and civilian Marines of MARFORCYBER, and the work they are doing to defend our nation from a growing and evolving threat.

Mission and Organization

As the Marine Corps Service component to U.S. Cyber Command, MARFORCYBER conducts full spectrum cyberspace operations. This includes securing, operating and defending the Marine Corps Enterprise Network (MCEN), executing DoD Information Networks (DoDIN) operations, conducting Defensive Cyberspace Operations (DCO) within the MCEN and Joint Force networks, and when directed, conducting Offensive Cyberspace Operations (OCO) in support of Joint and Coalition Forces. We do this to enable freedom of action in cyberspace and across all warfighting domains, and to deny the same to our adversaries.

As the Commander, MARFORCYBER, I wear two hats. I am Commander, MARFORCYBER, and I am the Commander of Joint Force Headquarters – Cyber (JFHQ-C) Marines. In these roles, I command about 1700 Marines, civilian Marines, and contractors across our headquarters and subordinate units. MARFORCYBER is comprised of a headquarters organization, a JFHQ-C, and two colonel led subordinate commands: Marine Corps Cyberspace Warfare Group (MCCYWG) and Marine Corps Cyberspace Operations Group (MCCOG). Through the JFHQ-C construct, we provide direct cyber operations support to U.S. Special Operations Command (USSOCOM).

In order to accomplish our mission, I organize operations along three lines of effort that I will highlight for you today. I use this framework to organize activities, allocate resources, grow capability, and measure our progress.

Secure, Operate, and Defend the MCEN

My first priority is to secure, operate, and defend the Marine Corps' portion of the DoDIN, the MCEN. We have continued to expand our definition of the MCEN by including all elements of the Commandant of the Marine Corps' IP space, which includes our many disparate networks that are owned and managed by different commands across the Marine Corps.

We accomplish this mainly through one of the two subordinate commands mentioned previously – the MCCOG. The MCCOG is responsible for directing global network operations and computer network defense of the MCEN. It executes DoDIN Operations and DCO in order to assure freedom of action in cyberspace and across warfighting domains, while denying the efforts of adversaries to degrade or disrupt our command and control.

With the increasing pace of operations in the cyberspace domain, the MCCOG, our primary DoDIN and Cyber Security Services Provider (CSSP), was designated an operational Command in December 2016. Internally, the MCCOG is re-organizing to more effectively fight in a high tempo environment and to better align to its operational command designation. Their re-organization will be complete this April.

Simultaneous with its designation, in August 2017, the MCCOG stood a Defense Information Systems Agency (DISA) mandated Command Cyber Readiness Inspection (CCRI) and a pilot Command Cyber Operational Readiness Inspection (CCORI), successfully passing both inspections and maintaining its certification as the Marine Corps' only CSSP. Additionally, during this same timeframe, MCCOG's Marine Corps Information Assurance Red Team (MCIART), the team responsible for assuming an adversarial role and testing our layered defenses across the Marine Corps, was recertified by the National Security Agency (NSA).

The Marine Corps views the MCEN as a warfighting platform, which we must aggressively defend from intrusion, exploitation, and attack. Recent real-world defensive cyberspace operations have informed and sharpened our ability to detect and eliminate threats on the MCEN. The operational posture to address vulnerabilities is critical as exploits are identified by USCYBERCOM or through adversary action. Recent operational successes include the replacement of more than 200 Virtual Private Network (VPN) Devices across more than 120 distinct sites in less than a 90 day period. In addition, recent real-world operations, such as responding to destructive and malicious global ransomware (WannaCry) and wiperware (Petya/NotPetya) events, have improved our ability to aggressively and successfully compress patching timelines and enhance our defenses in order to avoid exploitation.

While the MCCOG maintains a persistent capability to defend the Marine Corps' cyber battlespace, MARFORCYBER is continuously seeking methods to enhance the Service's defenses. Beginning in December, MARFORCYBER began augmenting the MCCOG's capability with other rapid and persistent defensive cyber resources that can quickly identify a threat, defend an area, eject adversaries, and recover from malicious activity. Though actively engaging an adversary in our battlespace is critical, securing the battlespace from attack is our first line of defense. Understanding this, we have adopted a philosophy of ruthless compliance with security measures across all elements of the MCEN. We are using every security action to increase our partnerships with other MARFORs and major subordinate commands to exercise command and control, and increase their understanding of the constant threat our adversaries pose in cyberspace. Cybersecurity is a team effort and it requires everyone to be engaged. We rely on the buy-in from our partners to ensure that the MCEN is properly protected.

We have improved network visibility and security by consolidating our legacy systems into a single homogeneous network. Consolidating domains reduces attack surfaces and improves our ability to identify and respond to threats. We are aggressively consolidating legacy domains, transitioning to the WIN 10 - operating system, and collapsing regional service desks to a single enterprise service desk. Our updates to each of these priorities are described briefly below.

Enterprise Service Desk. Since May, MARFORCYBER has been replacing regional service desks with a centralized, standardized Enterprise Service Desk (ESD) in Kansas City, Missouri to manage and monitor the MCEN, provide valuable insight regarding network trends, and rapidly respond to warfighter needs. The ESD is under the operational control of MARFORCYBER. While consolidation is not yet complete, the ESD has provided the anticipated benefits of improved service and network visibility, complementing other defensive actions on the MCEN. Our next step is to establish the Alternate ESD in New Orleans, and procure the equipment for both ESD locations. The FY19 President's Budget requests the funding to continue to stand up the ESD.

Domain Consolidation and Elimination (DC&E). We are continue efforts to collapse legacy networks into a single, homogenous and secure network. Legacy networks increase the Marine Corps' cyber footprint and unnecessarily increase attack surfaces for adversaries. Eliminating these networks and consolidating them within the MCEN will provide much needed standardization, increase network visibility, and decrease the attack surface available to our adversaries. Out of 52 legacy domains, only 18 remain to be decommissioned. The largest program of record requiring migration is the Marine Corps Enterprise Information Technology Services (MCEITS), a system that provides collaboration, data exchange, and information access. Planning is underway to migrate MCIETS onto MCEN-N. We anticipate completing our DC&E efforts by September of 2019 however, additional actions are required to consolidate legacy networks onto the MCEN such as migrating public-facing webservers into demilitarized zones, consolidating data centers, and conducting Enterprise Infrastructure Modernization (EIM).

We are also participating in joint efforts to secure our networks, most notably by integrating into the Join Information Environment (JIE). Through JIE, the Marine Corps will install Multiprotocol Label Switching as part of the Joint Regional Security Stack (JRSS) project and will standardize transport while improving security. In addition, the Marine Corps continues working with Joint Force Headquarters –DOD Information Networks (JFHQ-DODIN) to modernize infrastructure and comply with standards that protect our public-facing systems to reduce unnecessary and outdated public facing system, and harden and PKI-enable the remaining. Upgrades to the equipment and standards that safeguard our public-facing websites are underway to ensure we remain connected to the general public and industry while maintaining the latest in cybersecurity protections.

Windows 10. The Marine Corps continues its efforts to transition its Microsoft Windows end user devices to the Windows 10 (WIN 10) operating system (OS), effecting well over 100,000 devices on the unclassified network alone. In order to accomplish this task, MARFORCYBER exercised command and control relationships with Tier III Commanders and MARFORs to synchronize effort and resources, engage commanders across the force, and track progress. The

Service leadership has supported our efforts; and we have been providing periodic updates on progress and compliance to the Assistant Commandant of the Marine Corps. Our WIN 10 transition is currently on plan to meet 31 March deadline established by DoD.

Cyber is a dynamic, competitive environment, and we are continually responding to the increasing capability and capacity of our adversaries. We are improving our ability to understand system data and identify vulnerabilities. Through participation in various joint exercises, we continuously affirm that treating cyberspace as a contested warfighting domain is essential to our ability to rapidly identify and defeat an adversary. During Exercise Pacific Sentry, a bilateral exercise led by U.S. Pacific Command and linked to U.S. Strategic Command and USCYBERCOM headquarters' exercises, we identified several key stakeholders and owners of Marine Corps information repositories who must aggressively defend themselves in cyberspace in order to provide essential, service level activities. Our experience during real-world operations and training exercises has demonstrated that many commands and processes within the Service that have historically been considered administrative in nature must operationalize in order to function in a contested cyberspace domain. For example, our partners in cybersecurity inside the Service include acquisition commands and data owners. In cyberspace, the Supporting Establishment must respond with the same readiness and agility as the warfighting element.

Moving forward, and in response to the National Defense Strategy, we must build the objective network capable of fighting and winning against a peer adversary. We are participating in efforts to shape our battlespace within the Service by designing a more defensible architecture. The Objective Network is a service-level capability that spans all war-fighting functions and enables operations across all domains. The Objective Network must be deployable and resilient to support command and control functions throughout the Marine Air Ground Task Force (MAGTF) in a contested, disconnected, intermittent, and low bandwidth environment. To operate in this environment, the network must adapt to conditions and optimize performance, while reducing detection and vulnerabilities.

The objective network is essential to "make sense" of the cognitive domain, where enterprise and local resources feed critical thinking to drive commander's decision-making and enable information operations. Artificial Intelligence (AI) is the core element in accomplishing this in near-real time. An interconnected family of MAGTF AI systems share priorities, monitor the network, learn patterns, and inform human decision making. This enables AI to manage hardware and software components, route network traffic, and reduce the electromagnetic footprint. The result is a resilient command and control network that supports the warfighter even in the most austere environments.

Provide a Cyberspace Warfighting Capability

My second priority supports our responsibility to provide ready, capable cyber forces to USCYBERCOM's Cyber Mission Force.

The Marine Corps is responsible for 13 of USCYBERCOM's 133 Cyber Mission Force (CMF) teams: one National Mission Team (NMT), eight Cyber Protection Teams (CPTs), three Combat Mission Teams (CMT), and one Cyber Support Team (CST). These 13 teams are aligned against USCYBERCOM (Cyber National Mission Force), USSOCOM, and Marine Corps missions.

Three of the eight CPTs are service retained and oriented to service missions, (23% of the total Marine Corps CMF).

I am happy to report that, as of January 2018 and ahead of schedule, all of our 13 teams have reached FOC. All teams are fully engaged in supporting the mission. Although we have met FOC criteria, our work is not done. We have shifted our focus toward sustaining and improving our team readiness.

To increase readiness, improve effectiveness, and address retention of cyberspace operators, the Marine Corps recently established a Cyberspace Occupational Field. We have learned a great deal in the past several years about the training, clearance, and experience requirements across the cyber mission force. We know that in order to be effective, we must retain a professional cadre of cyberspace warriors who are skilled in critical work roles, and we know that many of our Marines desired to remain part of the cyber work force. We intend to begin assigning Marines to the cyberspace MOS on 1 October 2018. This will significantly improve both readiness and retention of the cyber force, and allow us to develop their skills throughout their careers.

I would like to thank Congress for authorizing the Marine Corps to grow its structure by 1,000 earlier this year to 185,000. Our growth in cyber is consistent with the Commandant of the Marine Corps' request to expand our ability to operate in the Information Environment and build capabilities that allow the Marine Corps' to increase its emphasis on maneuver in a cognitive sense, expanding our employment of combined arms to the domains of cyberspace.

The MCCYWG is our colonel led command that is responsible for identifying capability requirements, training, certifying, and sustaining readiness for our CMF teams. While they are currently minimally staffed, my vision for this command is to develop it into the centerpiece for advanced cyber warfare training, tactics, and certifications to support Marine Corps cyber forces. The Commandant of the Marine Corps recently approved growth for the MCCYWG to enable this vision in support of joint CMF and Marine Corps cyber units.

While building the CMF, members of the MARFORCYBER staff were dual-hatted as the Joint Force Headquarters staff. This year, the increasing pace of cyberspace operations demanded that we resource a separate, standing JFHQ-C. This JFHQ-C provides planning, targeting, and intelligence support to supported commanders, synchronizes execution of cyberspace operations, and provides command and control for CMTs and CST.

In May I updated you regarding the development of the Joint Force Headquarters – Forward, which was intended to integrate cyberspace operations with USSOCOM's global operations. Since then, the Secretary of Defense, through USCYBERCOM, instructed all Service Cyber Components to rename this organization the Cyberspace Operations – Integrated Planning Element (CO-IPE) and to complete an implementation plan no later than March of this year. We have been working through both USCYBERCOM and USSOCOM to identify and satisfy requirements in the most efficient manner possible.

In addition to the five Marines already at USSOCOM headquarters, we begun to build the CO-IPE across USSOCOM organizations worldwide and look to complete the civilian hiring for a total 26 civilians by October of this year. We have also been working within the Service to

increase our uniformed CO-IPE staff, with an increase of 13 Marines required to meet our staffing goal by the end of FY20.

As with all other domains, the Marines continue to be "First to Fight" in cyberspace. Our CMTs working in support of Joint Task Force Ares have conducted multiple, large-scale operations to support U.S. Central Command (USCENTCOM) and Combined Joint Task Force – Operation Inherent Resolve. We have also expanded our support beyond the CMTs to include cyberspace operations planners working at multiple locations both overseas and here at home with partner organizations. I currently have numerous Marines deployed to locations in both USCENTCOM and USAFRICOM, planning and integrating cyberspace operations into ongoing activities. We are also working within the Service to integrate cyberspace effects and planning into other domains. We recently deployed a Marine cyberspace planner to Afghanistan to assist the Marines in Helmand Province as Task Force South West executes their advise and assist mission with our Afghan partners. Through my deployed personnel, we are bringing cyberspace operations to the tactical edge of battle, while at the same time generating cyberspace experience and expertise within operational units outside of USCYBERCOM. These experiences will allow operational planners to adapt the emerging cyberspace capabilities in such a way that we can incorporate cyberspace operations at all levels of conflict across the full range of military operations.

We continue to improve on the Marine Corps' investment in specialized tools for defensive cyberspace operations. The Deployable Mission Support System (DMSS) hardware and software tools comprise the weapons system CPTs use to meet any mission they may be assigned, from readiness and compliance visits to incident response or Quick Reaction Force missions. The DMSS toolkit evolves with the threat and is continually revised and upgraded to ensure CPTs have the most up-to-date toolkit available for a dynamic cyberspace operations mission set. MARFORCYBER is also working to develop a DMSS-like toolkit for employment by the Service's Defensive Cyber Operations – Internal Defensive Maneuver (DCO-IDM) Companies, which will provide an organic defensive cyberspace capability to Marine Expeditionary Force (MEF) Commanders within the newly established MEF Information Groups (MIG). MARFORCYBER is currently finalizing the engineering and procurement of third generation DMSS 3.0 kits, the first of which is scheduled to be delivered in late FY18. Revisions in version 3.0 include: reduction in overall size of the system to allow for increased transportability on commercial flights, updated suite configuration to allow for split-based operations, leveraging reach-back capability to shared resources at a central location. We are working within the budget to address associated sustainment and operational support infrastructure.

We have established relevant operational capability in support of the warfighter and continue to experience consistent growth in operational capability and ability to deliver cyberspace effects.

Operationalize the Information Environment

My third priority is to add cyberspace warfighting expertise to the MAGTF and to enable operations in the Information Environment. Since our establishment in 2009, our Marines and civilians have implicitly understood the need to provide a high return on the Marine Corps' investment in cyber.

The Marine Corps Operating Concept (MOC) describes a future operating environment where Marines will fight with and for information, engage in a battle of signatures and be required to maneuver throughout networks even as we design networks that are maneuverable themselves. Last year, the Marine Corps developed a new force design to meet the needs of the MOC. This effort, called Force 2025, includes a DCO-IDM company and electronic warfare company for each MEF within the MIG. The DCO companies will provide MAGTF commanders with a trained and organized capability to conduct activities as maneuver elements for deployed networks, data stores and weapons system. As an element of the aforementioned MEF Information Group (MIG), the DCO-IDM Companies will support the defense of MAGTF key terrain in cyberspace and maintain a commander's ability to command and control. Their primary function will be mission assurance actions such, as actively hunting for advanced internal threats that evade routine security measures, performing incident response actions, and performing digital forensics.

MARFORCYBER continues to lead the DCO-IDM Training Pilot Program, which will inform the DCO-IDM Company concept of employment. We recently hosted DCO-IDM Training at MARFORCYBER, which included command leadership from all three MIGs as well as members of the DCO-IDM Companies. The pilot training included hands on training for the Marines of the DCO-IDM Companies provided by MCCWYG as well as training for MIG leadership on employment, authorities, capabilities, and command and control. In addition, our Service retained CPTs remain engaged with the DCO-IDM Companies and continue to provide training opportunities. Members of DCO-IDM Companies have accompanied our Service CPTs during real-world operations and this partnership continues today.

To increase cyber readiness across the Service, we continue to emphasize the role of the Commander in the security and defense of the MCEN, and are conducting Cyber Readiness Visits at commands throughout the Marine Corps to identify cyber key terrain, assess readiness and culture, and bolster our defenses. As the Marine Corps' cyber career field comes online, we will aggressively build cyber operators to ensure the MAGTFs, bases and stations have the expertise and capacity to enhance cyber readiness not only at MARFORCYBER, but across the Marine Corps.

We have accomplished much in a short period working within the construct of these lines of effort, but still much work to do.

Cyber Workforce Management

Since my last testimony in May, Headquarters, Marine Corps has approved my request to grow MARFORCYBER capability and capacity. We are now working on implementation as we nearly double the size of the command, adding more than 500 additional personnel, both uniformed and civilian. This growth includes increased capacity at the MARFORCYBER Headquarters staff, increasing the size of MCCWYG to focus on improving our readiness through improved training and application of lessons learned across the Marine Corps, and creating a fully staffed JFHQ-C. This growth is programmed to occur over the next 5 years, starting this year and ending in FY 22. Our growth is in-line with the Commandant's vision and Future Force 2025.

At MARFORCYBER we have more than 60 reservists integrated into the command, both as mobilized Marines who are working 365 days a year to support our mission, along with part time

drilling Marines who come in periodically over the course of the year for both individual training periods and two week active duty training periods. Both groups of reservists provide one of the three functions; MARFORCYBER staff augmentation, support to MCCYWG, and support to joint, academic, and experimental activities. Over the last year our Marine reservist have made numerous contributions, including filling key roles in the MARFORCYBER staff, as well as augmenting USCYBERCOM in support of operational requirements. The Marines providing reserve support to the MCCYWG leverage skills they have acquired both in Service and from their civilian work environments. They support and augment CPT activities based on identified skill gaps. Recently, one of our CPTs had a scheduled mission and a last minute personnel gap was identified, and with 48 hours, a Reservist with the requisite skills volunteered to support the mission. This is just one example of how our Reserve Marines are a force multiplier in the defense of the MCEN.

Marine Forces Reserve (MARFORRES), in conjunction with the current effort to increase Active Component (AC) DCO capability and capacity, is developing a Reserve Component capability to augment, reinforce, and sustain AC MEF DCO requirements. The primary capability will be the activation and phased build of two Selected Marine Corps Reserve (SMCR) DCO-IDM Companies. These companies will be structurally similar to their AC counter-part companies and will most often be deployed and employed at the team level. MARFORRES' vision is to create meaningful opportunities for the population of Marines who leave active service, and to capitalize on their success and credentialing as civilians in the IT sector.

On the civilian side, the Office of Personnel and Management approved an increase in MARFORCYBER's recruitment and retention incentives from 25% to 50%. These additional incentives have assisted in hiring and maintaining critical cybersecurity civilian billets within MARFORCYBER. This increase provides us the ability to negotiate with the workforce, gaining ground against the private sector's ability to offer more money and incentives. In addition, we are participating in the DoD's Cyber Excepted Service (CES) Personnel System. The CES is a personnel system aligned to both Title 10 and Title 5 provisions that support the human capital lifecycle for civilian employees engaged in or in support of cyber-related missions. The implementation of this new personnel system will occur over three phases, with Phase II beginning in January of this year for the Service Cyber Components and, extending over a two year implementation process.

Policy that limits the recruitment of recently retired or separated service members that are cleared and fully trained has become substantially more difficult after the expiration of the policy suspending the 180-day cooling off period required before taking a government position. While there is a waiver process for uniquely qualified candidates, we have found that the waiver process itself is cumbersome and not timely, approaching 180 days in many cases. We are working with key stakeholders to help streamline the waiver process, which would help decrease the wait time in getting qualified personnel on board. To ensure that we are not unnecessarily losing our homegrown talent, the cyber workforce should be waived from this requirement.

As we continue to increase our capability and capacity, we look forward to occupying our new headquarters building on NSA's campus. I want to again take the opportunity to thank you for

the Military Construction funding that enabled the development of our new headquarters. When I was last before you in May, I updated you on the development of this new operational headquarters facility, designed to meet the demands of our increased mission. Previously referred to as the East Campus Building- Marine Corps, I am pleased to inform you that we have received approval from within the Service and USCYBERCOM to name our new facility after an American hero, Colonel Alva B. Lasswell. Colonel Lasswell was a World War II cryptologist credited with translating an intercepted message that revealed Japan's planned attack on Midway Island. Colonel Lasswell's work enabled Admiral Nimitz to appropriately plan history's first great carrier battle at Midway, a turning point of the war in the Pacific Theater.
This building is much more than just new administrative offices – it will serve as the Marine Corps' premier cyber warfighting platform, and will provide full spectrum cyberspace operation capabilities. We are on schedule to complete our move in to the Lasswell Building by 4th quarter of FY18, and we anticipate a dedication and ribbon-cutting ceremony to be held sometime this spring.

Conclusion

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to testify before you today, and for the support that you and this Committee have provided our Marines and their families.

I am incredibly proud of the strides we have made in operationalizing cyberspace in support of the MAGTF and joint warfighter since I was last before you in May, but we have not succeeded alone. Our successes have come from a growing network of partnerships across the Service, the Operating Forces, government, industry, and academia. Cyberspace is a team effort and we are quickly gaining momentum and buy-in to build a more capable, ready force that is prepared to fight –and win- tonight in the cyberspace domain.

I look forward to continuing this dialogue and working with members of this subcommittee in the future.