NOT FOR PUBLICATION UNTIL RELEASED BY
THE SENATE ARMED SERVICES COMMITTEE
CYBERSECURITY SUBCOMMITTEE

STATEMENT BY

MAJOR GENERAL LORI E. REYNOLDS

COMMANDER

MARINE CORPS FORCES CYBERSPACE COMMAND

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY

CYBER POSTURE

1ST SESSION 115TH CONGRESS

MAY 23, 2017

Major General Loretta E. Reynolds:

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 Master's 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, on behalf of the Marines, civilian Marines, and the families of U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER), I thank you for your continued support of the important work we are doing to secure, operate, and defend the Marine Corps Enterprise Network (MCEN) and defend the nation in cyberspace. I welcome this opportunity to highlight what our Marines are doing in the cyberspace domain and how we are shifting our focus from building the command to operationalizing, sustaining, and expanding capabilities in this warfighting domain. I am pleased to be sitting alongside my colleagues from the other Service Cyber Components of the United States Cyber Command (USCYBERCOM).

I am humbled everyday by the tenacity, professionalism, and commitment to mission success displayed by my team. It gives me great pride to highlight the many accomplishments of the Marines and civilian Marines of MARFORCYBER, and the work they are doing in support of warfighting and in defense of our nation.

It will come as no surprise to the members of this committee that we face a growing cyber threat - one that is increasingly persistent, diverse, and dangerous. Malicious cyber activity from both state and non-state actors continues to intensify and every conflict around the world includes a cyber dimension. The traditional fight we have envisioned across the domains of air, land, sea, and space has expanded to the cyber domain. The United States' technical superiority is not yet established in this domain: we have to earn superiority in each fight. We can never take our superiority for granted. Our enemies will test us.

This year we established MARFORCYBER's motto – *Semper in Proelio*. It is Latin for "Always in Battle." This is the reality of cyberspace. The American people rightfully expect their Marines to fight our Nation's battles and win – always, including in the domain of cyber. We work hard each and every day to ensure we are prepared to fulfill this expectation.

Mission and Organization

As the Marine service component to U.S. Cyber Command, MARFORCYBER conducts full spectrum cyberspace operations. That includes operating and defending the MCEN, 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 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). We are currently in the process of developing and manning a Joint Force

Headquarters – Forward, which is part of an effort to meet the growing demand of cyber operations throughout USSOCOM's global operations.

Within the MARFORCYBER headquarters, we currently have 189 authorized billets for Marines and 32 authorized billets for government civilians. We have an additional 65 authorized billets for contract employees. In a field where technology is paramount, our people continue to be our most valuable resource and greatest strength. Simply put, they represent the very best our nation has to offer - they are patriots, who are doing the arduous and necessary work to defend against increasingly capable adversaries.

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 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.

This past December, the MCCOG was activated during a re-designation ceremony from the former Marine Corps Network and Operations Security Center (MCNOSC). This re-designation was not simply a name change. The missions and roles assigned to the MCNOSC transitioned from that of a Supporting Establishment command to that of an Operational Force command apportioned to U.S. Strategic Command (USSTRATCOM).

The Marine Corps views the MCEN as a warfighting platform, which we must aggressively defend from intrusion, exploitation, and attack. Cyberspace operations favor the attacker, and our operational dependencies require us to conduct a formidable, continuous defense. Real-world defensive cyberspace operations have informed and sharpened our ability to detect and expel threats on the MCEN. Since May 2016, the MCCOG has responded to 4,050 events on the MCEN. These events include unsuccessful attempts to access the network, non-compliance with security standards, reconnaissance of the network, and explained anomalies (configuration errors). This number encompasses only the events that require our attention and further analysis. There are thousands of events that occur on the network daily that are blocked and contained by our network defenses and filters.

Our priorities for improving our defenses this year include actions to flatten the Marine Corps network and improve our ability to sense the environment, harden the network through increased endpoint security, and decrease incident response time. To do this, we are aggressively seeking to consolidate legacy domains, implement a comply to connect capability and the WIN 10-operating system, and collapse regional service desks to an enterprise service desk. Each of these priorities are described briefly below.

Network Access Control, Compliance, and Remediation (NACCR). NACCR provides defense in depth by positively identifying devices that attempt to connect to our networks, ensuring the device is compliant with the latest set of security updates, and, if non-compliant, NACCR initiates quarantine and remediation actions.

Enterprise Service Desk. We are transitioning eight regional service desks into a central, standardized Enterprise Service Desk (ESD) in Kansas City, Missouri. The ESD will be under the operational control of MARFORCYBER. Users' requests for IT support and incident response, once centrally managed, will provide valuable insights into trends on the network. Long term benefits will include supporting a top down governance structure, increased efficiency in supporting the warfighter, and providing a holistic view of the network that informs and complements defensive actions on the MCEN.

Domain Consolidation. In order to flatten, harden, and secure the network, we must have full visibility of all networked assets. We are undertaking efforts to bring remaining disparate legacy networks into a homogenous and secure network. Legacy networks contribute to the Marine Corps' cyber footprint and unnecessarily increase attack surfaces for adversaries. This deliberate effort for domain consolidation will provide much needed standardization and increase the cybersecurity posture of the MCEN.

Windows 10. The Marine Corps is transitioning its Microsoft Windows end user devices to the Windows 10 (WIN 10) operating system (OS). WIN 10 OS will improve the Marine Corps' cybersecurity posture, lower the cost of information technology (IT), and standardize the Marine Corps' IT operating environment. The WIN 10 OS has numerous embedded security features that earlier Windows OS's lack. These features include protection such as encrypting hard drive data while powered off or preventing the execution of unknown system commands.

Like the Internet itself, many of our Programs of Record and warfighting systems were not built with security in mind. To combat these vulnerabilities, we are reviewing each one to determine how we can improve security. We have also conducted a review of all vulnerable end of life hardware and software on the network and developed expedited strategies to upgrade, consolidate or remove systems that cannot be adequately hardened. Projects that focus on auditing, analysis and tracking of cyber events and anomalous activity have been developed and implemented to improve our situational awareness of system status and cyber monitoring capabilities. Programs that test and audit our defensive posture are continuously reviewed for relevance and improvement to address the changing cyber threat environment and support the intelligence operations cycle on a shortened timeline. Cyber is a dynamic, competitive environment, and we are continually responding to the increasing capability and capacity of our adversaries.

As we have built Cyber Protection Teams (CPT), we have employed them across the MCEN. This year, our CPTs have conducted named cyber operations to include focused internal defensive maneuver missions (IDM), ensured security of Personally Identifiable Information (PII) repositories, and completed security enhancement missions for cyber key terrain, countering known threats to the network. In all DCO activities, the Marine Corps consolidates findings and actionable lessons for dissemination to the broader operational community.

We are making efforts to better understand system data, and have employed Service aligned CPTs to harden Service PII repositories. In 2015, MARFORCYBER began efforts to secure PII repositories across the service. The MCCOG and Service CPTs assessed the security posture of our 40 largest PII repositories. While the overall security posture of our systems was within established standards, we identified areas for improvement we needed to address. Our Service aligned CPTs conducted on-site visits to several repositories that were deemed critical high risk. There, we identified and remediated vulnerabilities and trained system owners and administrators. We continue efforts to ensure these systems maintain the highest levels of security.

We have identified a requirement for a more robust MCCOG Continuity of Operations (COOP) capability. The MCCOG COOP is effectively a MCEN COOP capability. MCCOG lacks the ability to comply with DoD Directive 3020.26 of 9 Jan 2007 requiring up to 30 days Mission Essential Services and Functions performance for no-notice events. The Marine Corps IT Center (MCITC), located in Kansas City, Missouri, is the recommended COOP site, allowing us to leverage available space and integrate with other MCCOG operations already at MCITC. We have conducted thorough analysis and research to develop an effective COOP capability, but currently lack the financial resources to put our plan into action.

We are participating in efforts to shape our battle space by designing a more defensible architecture. As we move toward implementing the Joint Information Environment, we are also working to unify and centralize our network to better see, understand, and defend the MCEN. We are integrating and standardizing cyberspace threat reporting, intelligence production and analysis to better inform commander's situational awareness and decision making. Our network must be resilient, redundant and interoperable, and extend from garrison to the tactical edge of battle. In other words, we need a seamless MCEN that provides a defensible capability providing enterprise services from "fighting hole to flagpole." We are moving out in this direction.

Provide a Cyberspace Warfighting Capability

My second priority supports our responsibility to provide ready, capable cyber forces to USCYBERCOM. Creating this capability in a new command is a tremendous undertaking. We are on track to provide our Combat Mission, Cyber Protection, National Mission, and Combat Support teams in time to meet USCYBERCOM Full Operational Capability (FOC) requirements.

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).

Of our 13 teams, nine teams have reached and four teams remain at Initial Operating Capability (IOC). All 13 teams are scheduled to reach FOC in FY 18. It's important to note, that all 13 teams designated as having reached IOC are employed against real-world problem sets and are fully engaged in supporting the mission. It is also important to note that achieving FOC is also not an indication that work is done. We must continually ensure we are training and sustaining the force to ensure we remain agile, adaptable, and ready to defeat all enemies.

To that end, we are moving forward with the creation of 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 desire to remain part of the cyber work force. The Commandant has told us to move out, and we are planning with Headquarters, Marine Corps (HQMC) to design a cyberspace occupational field to address offensive and defensive team readiness requirements. We intend to begin assigning Marines to the cyberspace MOS in FY18. This will significantly improve both readiness and retention of the force.

In the spring of 2016, we activated the MCCYWG. This new command is a colonel led command with the responsibility for identifying capability requirements, training, certifying, and sustaining readiness for our CMF teams. In the future, my vision for this command is to develop it into one of service as the Cyber Warfighting Center for the Marine Corps, where it will provide standardized advanced cyber training and certifications that support Marine cyber training and readiness across the Corps.

While building the CMF, members of MARFORCYBER were dual-hatted as the Joint Force Headquarters staff. This year, the pace of cyber operations demanded that we begin to man a standing JFHQ-C. The JFHQ-C provides the planning, targeting, intelligence and cyber execution support to supported commanders, and provides command and control for CMTs and CST. This summer, we will begin hiring JFHQ staff who will be positioned forward and integrated into USSOCOM planning and intelligence processes in Tampa, Fort Bragg, and across Theater Special Operations Commands.

This year the Marine Corps continued its initial 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. This year, we championed an ability to conduct split based operations with the DMSS, enabling the CPT lead to forward deploy a small element and push information back to a home station "war room" for remote analysis and remediation. This initiative and concept of employment will reduce deployed time and costs and increase our ability to collaborate more freely with other CPTs or across the mission force.

We are rapidly establishing relevant operational capability in support of the warfighter. We have experienced tremendous growth in operational capability over the past year as we have fully supported the delivery of operational cyberspace effects under Joint Task Force Ares, a USCYBERCOM led effort designed to support C-ISIS efforts in U.S. Central Command (USCENTCOM). Our Joint Force Headquarters is providing relevant support to more fully integrate planning cyber operations, intelligence and fires, and we continue to refine procedures with each exercise and operation we support. On the defense, our CPTs are contributing to Cyber National Mission Force priorities around the globe, and at USSOCOM. Across USCYBERCOM, Marines are at the point of friction, increasingly relevant and eager to contribute to the fight.

We are also active participants with other Service components and USCYBERCOM in a variety of new processes, infrastructure and tool development, acquisition initiatives, training transition,

and Tactics, Techniques and Procedures (TTP) development for the CMF. We know we must continually adapt, innovate, and change to meet future threats.

Add Value to the MAGTF

My third priority is to add cyberspace warfighting expertise to the Marine Air Ground Task Force (MAGTF). Our Commandant, General Neller, understands the necessity to move forward quickly to build MAGTF capability to operate in all five domains. This is not the fight of the future, but the current fight we are in right now. Consistent with our Commandant's guidance, we want to develop 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.

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. In 2010, we began participating in Service training, exercises and concept development to institutionalize cyber across the Service, and have built momentum ever since. Cyberspace operations are now codified in scenarios at Marine Corps Tactics and Operations Group, Marine Corps Logistics Operations Group, and Marine Aviation Weapons and Tactics School, and the Marine Expeditionary Forces (MEFs) better understand the integration of cyber through our participation in MEF Large Scale Exercises. For the first time, this Fiscal Year we will have supported a training exercise within each MEF, our major warfighting commands. In addition, we recently concluded a mission in support of a Special Purpose MAGTF in the USCENTCOM AOR. Commanders across the Marine Corps and combat commands have seen the capability our defensive teams bring to the fight. Across the board, the demand signal for Marine Corps cyber operators and capability is high, and increases with each successful mission.

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 Design 2025, includes Defensive Cyber Operations-Internal Defensive Measures (DCO-IDM) companies and electronic warfare companies for each MEF. 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 MEF Communication Battalion, the DCO-IDM Companies will support the defense of MAGTF communication networks 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 is leading the DCO-IDM Training Pilot Program this month, which will inform the DCO-IDM Company concept of employment.

The Electronic Warfare companies, built inside our Radio Battalions, will employ similar intelligence, targeting and effects generation TTPs as offensive teams and will provide full spectrum electromagnetic support capability to the MEF commander.

To increase cyber readiness across the Service, we have emphasized 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 establishes the cyber career field for Marines, 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.

As we have transitioned from building the CMF to sustain readiness of the CMF, we are looking more carefully at how we retain manpower, prioritize training, ensure that our tools are current and sufficient to counter the growing threat, and whether we will have sufficient infrastructure, tools and facilities available for the force. We look forward to working more closely with Congress to address needs as we identify them.

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

Cyber Workforce Management

MARFORCYBER is conducting a multi-year, Service-integrated, bottom-up approach to grow both our headquarters element and the MCCYWG headquarters, which includes growth within manpower, training, facilities and equipment. Our growth is in-line with the Commandant's vision and Future Force 2025.

Since our last testimony before the House Armed Services Committee in March of 2015, we have initiated plans to significantly increase our headquarters staff. While MARFORCYBER has seen manpower growth in support of our CMF, as directed by the Secretary of Defense, we have not seen growth for the headquarters element that supports the CMF. Growth will require resources to hire personnel for the enabling operational and strategic headquarters staff, and for facilities where we can train and employ them.

MARFORCYBER was established with an initial staff of eight personnel. In 2011, we received additional personnel when the Service conducted a Force Structure Review. Since that time, the mission of MARFORCYBER has changed several times, including the requirement to grow a JFHQ-C, and our alignment to support USSOCOM. Concurrently, USCYBERCOM has developed new processes, working groups and planning teams to address the growing mission and relevance of cyberspace, while we have seen a steady increase in capability of adversary nations. In short, the scope of our mission has increased substantially, exceeding our existing capacity, and we have identified significant growth requirements to HQMC. One of the key requirements to grow and maintain an effective CMF is our ability to hire and retain the highest quality cyberspace professionals.

In workforce management, we are being challenged by the policy issues discussed below as well as the increasing demand for workers with cyber experience in industry and government. Private industry remains an attractive prospect for our cyber personnel with salaries and incentives we cannot compete with. On the uniformed side, we are successfully leveraging our Reserve forces to help close manpower gaps. This capability has given us a tremendous boost, with Reservists agreeing to come on orders for anywhere from one to three years.

The establishment of the cyber career field outlined earlier is one way we are addressing this challenge. We surveyed a sample of our CMF and found that 54% of respondents indicated that his or her work role was the most important consideration concerning re-enlistment with only 38% of respondents indicating pay was the most important (8% were undecided). Marines want to stay cyber Marines, and we will soon allow them the opportunity to do that.

The Marine Corps also has other initiatives underway to help address the manpower challenges identified above. We are scheduled to brief HQMC in early June on manpower growth requirements for both the MARFORCYBER and MCCYWG Headquarters. Our requirement is for additional intelligence professionals, logistics and administration personnel, network experts, acquisition and contract management teams and tool development experts. The Service is conducting a holistic analysis to ensure our growth is realistic, valid and complete.

On the civilian side, policy that exempted cyberspace positions during the recent hiring freeze was helpful in supporting our civilian workforce growth. However, the recruitment of recently retired or separated service members that are cleared and fully trained has become substantially more difficult after the expiration of policy suspending the 180-day cooling off period required before taking a government position.

We are well into the development of a new headquarters building for MARFORCYBER designed to meet the demands of our increased mission. I want to thank you for the Military Construction funding that enabled the East Campus Building – Marine Corps (ECB-MC) project. ECB-MC is a 148,000 square foot, 550 seat building that will provide full spectrum cyber operation capabilities. The project broke ground in October 2015 and the steel work "topped out" in November 2016. MARFORCYBER and our partners have developed a phased turnover plan to facilitate the fit-up of the building's complex systems and we expect the final turnover of spaces in December 2017. Assuming the construction and fit-up schedule is maintained, we expect to move MARFORCYBER into the new building during the 4th quarter of FY 18. This space is much more than administrative offices. It will serve as the Marine Corps' premier cyber warfighting platform.

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 have outlined just a handful of examples that share how our Marines are leaning in to increase cyber capability and capacity across this command and the Marine Corp through our lines of effort to secure, operate, and defend the MCEN, provide a warfighting capability, and provide value to the MAGTF. The success of these efforts depend on our Marine Corps cyber team – a team made up of warfighters, who are dedicated to their warrior craft. They are professional, competent, and committed to mission success. Simply put, they represent the very best.

I look forward to continuing this dialogue in the future and would be happy to take your questions.