NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED SERVICE COMMITTEE

STATEMENT OF

LIEUTENANT GENERAL GEORGE J. FLYNN

DEPUTY COMMANDANT

FOR

COMBAT DEVELOPMENT AND INTEGRATION

BEFORE THE SUBCOMMITTEE ON

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

OF THE

HOUSE ARMED SERVICES COMMITTEE

CONCERING

OPERATING IN THE DIGITAL DOMAIN: ORGANIZING THE MILITARY

DEPARTMENTS FOR CYBER OPERATIONS

ON

SEPTEMBER 23, 2010

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED SERVICE COMMITTEE

Chairwoman Sanchez, Ranking Member Miller, and distinguished members of the subcommittee, I am honored to appear before you today. On behalf of all Marines, I want to thank you for your continued support to our Marines and their families. I appreciate the opportunity to discuss the Marine Corps Cyberspace Command (MARFORCYBER) with you. The Marine Corps has taken a very deliberate approach to the establishment of MARFORCYBER.

I would like to begin by providing you an overview of our view and approach to cyberspace as well as a synopsis of the support we provide to US Cyberspace Command (USCYBERCOM). I will also expand on our known and anticipated challenges; planning efforts; and finally, where I believe help is needed for execution of our cyberspace mission.

Cyberspace View and Approach

Cyberspace is many things to many people: a marketplace, a schoolyard, a library, a neighborhood, a base for criminal activity, a command and control infrastructure. The Marine Corps has established the MARFORCYBER to focus its cyber efforts. In coordination with USCYBERCOM, MARFORCYBER will plan, coordinate, integrate, synchronize and direct *defensive* cyberspace operations to *preserve* the Marine Corps ability to use and function within the Marine Corps Enterprise Network (MCEN).

The Marine Corps is continuing its deliberate approach to cyber by exercising diligence in the standup of effective cyber organizational structures and the application of both “pure” and “related” cyber resources. Pure cyber resources are comprised of an operational headquarters activity, the MARFORCYBER Command Element; the Marine Corps Network Operations

Security Center (MCNOSC); and finally, the Marine Corps Cryptologic Support Battalion's (MCSB) Company L. Related cyber functional resources are information technology Marines who support or affect the MCEN but are not directly within the MARFORCYBER. The Marine Corps is currently reviewing the application of these resources.

In building our cyberspace capabilities, the Marine Corps will dedicate approximately 800 personnel to the "pure" cyber workforce. The keystone to this relatively small workforce is the vision that all Marines who access and use the MCEN will become Cyber Marines. It is through their collective diligence that the Marine Corps will defend the MCEN, mitigate or eliminate vulnerabilities, and fortify our defensive posture.

As the cyber workforce is recruited, training will be essential to their ability to defend and support cyberspace operations. A typical Cyber Marine will require two years of classroom and on-the-job training to be proficient in cyberspace operations. The Marine Corps envisions a holistic, joint approach to cyber training. Accordingly, our Cyber Marines are attending and providing input to the Joint Cyber Analysis Course (JCAC) and the Joint Network Attack Course (JNAC). Defensive cyberspace resources encompass a number of cyberspace specialties, each with different training requirements.

Consistent with Secretary Gates' recent direction to create efficiencies across the Department by leveraging economies of scale in purchasing information technologies, MARFORCYBER envisions, and is advocating to USCYBERCOM and the other Service Components, a joint approach to equipping the force. Internally, the Marine Corps is currently focusing its cyberspace fiscal resources on Computer Network Defense through investments at the MCNOSC.

US Cyberspace Command Support

MARFORCYBER provides support to USCYBERCOM as the Marine Corps' Service Component. MARFORCYBER is actively engaged with USCYBERCOM at all levels of the organization. From the monthly Cyber Component Commander's Conference to daily interactions and operational planning teams, MARFORCYBER is supporting USCYBERCOM. Operationally, MARFORCYBER and MCSB Company L provide resources for National and Joint kinetic attack requirements; deployed forces in support of ongoing operations in Afghanistan; as well as, direct support to USCYBERCOM collaborative planning efforts.

The Marine Corps is undertaking a significant effort to define cyber capability and capacity. For capacity, the Marine Corps is trying to balance what it needs to do for the provision of cyber expertise and support to USCYBERCOM with its own cyber operational requirements. For capability, we are determining what resources will be required to sustain cyber operations across the cyber spectrum in support of both USCYBERCOM and Marine Corps operational requirements. These considerations together will determine the future shaping of the force, how we man, train and equip our Cyber Marines as well as deliberate preparations to cyberspace operations.

Challenges to Cyberspace Operations

There are operational challenges in cyber defensive activities. The challenges are emerging and not completely known at this time. Flexibility will be paramount to ensure mission and resource effectiveness while process development, doctrine and other modes of operation are developed, trained, and ingrained in our culture.

Being ready to operate successfully in an uncertain environment is a strength of your Marine Corps. Readying Marine Corps cyber forces is critical to success and our top priority. Readying our force includes recruiting, training, equipping and retaining the workforce. I would like to discuss with you the known challenges in each of these areas:

- *Recruiting*: We will achieve our FY10 cyber workforce recruiting goal using competitive enlistment bonuses for enlistment contracts with a minimum five year retention period. Existing Marine Corps policy limits maximum obligation periods to no more than five years. However, with a two year upfront training requirement, a longer service period is needed in order to achieve a return on investment.
- *Training*: As I have previously stated, the keystone to our small cyber workforce is the vision that all persons who access and use the MCEN will be critical to our cyber defense. Our challenge includes creating an acceptance throughout the Marine Corps that each person affects the cyber defensive posture of the Marine Corps. Additionally, as the cyber workforce grows and matures, another challenge will be to provide Marines a comprehensive roadmap for training and career development.
- *Equipping*: In order to be effective, Marines need to be properly equipped. Our cyber forces are no different. The cyber workforce must be equipped with the most appropriate and effective tools and capabilities. In our view, traditional acquisition approaches will likely not support the speed of cyberspace operations.
- *Retaining*: As the economy improves, the Marine Corps will compete for trained cyberspace personnel. Although the Marine Corps can offer these talented professionals something the civilian sector cannot – the opportunity to serve their country with pride, honor, and

distinction in a cutting edge role as a Marine – in some cases the lure of increased salaries and corporate titles/status will not be overcome.

We must be adaptive and provide our Marines with the tools they need to maximize their operational flexibility. To do this, we must remain vigilant and prepared. The threat in cyberspace is persistent, 24 hours a day, 7 days per week, and 365 days per year. With the support of the Congress, the American people, and industry we can ensure our Marines are ready now as well as in the uncertain future. I thank you for the opportunity to report on their behalf.