Rapid Cyber Acquisitions

Marine Corps Systems Command stakeholders in action

by Alan Stocks

>Mr. Stocks is a former Marine who flew CH-53s during DESERT SHIELD/DESERT STORM. He is currently a Program Analyst with Marine Corps Systems Command, supporting cyber issues.

Spurred by then-MajGen O'Donahue, Commander, Marine Corps Forces Cyberspace Command (MFCC), in April 2015, the CMC directed the Deputy Commandant, Combat Development & Integration (DC, CD&I), to establish a Marine Corps Cyber Task Force to operationalize the cyber domain. The task force directed USMC cyber stakeholders to seek disruptive improvements, and it specifically tasked Marine Corps Systems Command (MCSC) to improve cyber and information technology (IT) acquisitions responsiveness. MCSC wrote the acquisitions task, which stated,

> MCSC develops acquisition and procurement approaches which provide speed to warfighting capability while not sacrificing the discipline necessary to provide a unified, standardized, configuration-controlled Marine Corps enterprise network.

The Commander, MCSC, activated an MCSC Cyber Operational Planning Team (OPT) to address this task. Over three months and via the Marine Corps Planning Process, MCSC framed the cyber/IT acquisitions problem. Stakeholders at MCSC; HQMC Command, Control, Communications, and Computers (HQMC C4); Marine Forces Cyberspace Command (MARFORCYBER); the DC, CD&I; the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD, AT&L); the Deputy Commandant, Installations & Logistics (DC, I&L); the Deputy Commandant, Programs & Resources (DC, P&R); the Program Executive Office for Enterprise Information Systems; and at Naval Enterprise Networks (PMW 205) were asked the following questions:

- What is broken with the current cyber acquisitions process?
- How can we fix the cyber acquisitions process?
- How can your organization be part of the solution to fix the cyber acquisitions process?

The Cyber OPT developed fifteen problem statements touching on all aspects of the acquisitions process and addressed people, process/policy, organization, requirements, funding, procurement, sustainment, and governance. During course of action development, we applied only one criterion: courses of action must address at least one problem statement, have a measurable impact, and comply with laws, regulations, and policy. By June 2015, the Cyber OPT provided 26 recommendations to expedite cyber acquisitions, and within those 26 recommendations, there are 40 tasks that broadly fall into two categories based on their scopeof impact. There are ten cyber-specific tasks affecting MCSC cyber stakeholders, and there

Are there items of equipment that can be procured for our Marines more rapidly and efficiently? *(Photo by LCpl Rhita Daniel.)*

are 30 general acquisitions tasks affecting all of MCSC.

The MCSC changes are termed "Little A" acquisitions and are completed or are permanently instantiated within MCSC processes and continue to improve. Those applying to MCSC's cyber stakeholders are termed "Big A" acquisitions and are considered institutional by nature. Most of those external to MCSC are either not started or are delayed. The Cyber OPT also developed a rapid cyber acquisitions process with necessary authorities and adequate resources to address validated 30-day emergency and 180-day urgent cyber requirements.

The Commander, MCSC, submitted the MCSC Cyber OPT results to the DC, CD&I, who then brought them to the July CMC Executive Off-Site (EOS). The EOS accepted all 26 recommendations and subordinate tasks. In September 2015, the Commander, MCSC, issued a decision memorandum that identified a plan of action and milestones to work the EOS-accepted recommendations to improve cyber/IT acquisitions. The Commander also issued a decision memorandum establishing the cyber acquisitions team (CAT) to manage these acquisitions changes. MCSC directly supported external stakeholders in their execution of the Big A recommendations/tasks so as to generate an acquisitions tempo across all IT and ground weapons systems portfolios and the institution at large.

MCSC "Little A" Cyber Acquisitions Recommendations

People:

- Build and shape a cyber acquisitions workforce.

Process/policy:

- Create a cyber rapid response planning and fielding process with necessary authorities and adequate resources to address validated urgent requirements (analogous to the *MCWP 5-1* rapid response planning process).
- Define a cyber acquisitions process that identifies a single MCSC requirements entry point, determines if requirements are actionable, and accepts, prioritizes, and assigns it to an appropriate MCSC lead.
- Generate and maintain a comprehensive list of active contracts available to support cyber acquisitions, and, where necessary, create new contract vehicles to cover gaps.
- Develop a cyber acquisitions "playbook" that balances the operational with acquisitions risk and speed to delivery.
- Review internal processes/policies to reduce barriers, to include the external contract waiver process.
- Identify, document, and delegate decision authority commensurate with risk, and define the role of competencies.

Organization:

- Evaluate the organizational structure to gain the efficiencies and effectiveness of personnel, processes, and resources.
- Educate the acquisitions workforce on cyber as a warfighting domain.

Marine Corps "Big A" Cyber Acquisitions Recommendations

Requirements:

- Implement the CD&I requirement transition process (RTP) as the single Marine Corps source for sending cyber requirements to MCSC.
- The CD&I RTP will communicate prioritization of emergency (~30 days), urgent (~180 days), and deliberate cyber requirements to MCSC.
- Gain Marine Requirements Oversight Council's approval of the Marine Corps Enterprise Network (MCEN) unification plan to align requirements, funding, and acquisitions (CD&I: 90 days).

Funding:

- Establish year-of-execution funding strategies for unfunded cyber requirements (P&R/CD&I/MCSC: 30 days).
- Resource the program objective memorandum to support MCEN unification.
- The programs of record should include cyber requirements in program objective memorandum planning and submission (P&R/CD&I/MCSC: 90 days).

Procurement:

- Establish an approved product list, and have C4, intelligence, MCSC, MFCC, I&L, CD&I, and Operating Forces identify approved equipment and develop a method to acquire the list's items (C4 by 31 Dec 2015).
- Establish a MCSC liaison office to MARFORCYBER (MCSC/MFCC: 90 days).
- Eliminate duplicative engineering processes at MCSC and Marine Corps Network Operations and Security Center (MCNOSC) (MFCC/MCSC: 90 days).
- Define criteria that determines HQMC I&L and MCSC's contracting responsibilities for MCNOSC requirements, and consider embedding a contracting team at the MCNOSC (I&L/MCSC/MFCC: 90 days).

Sustainment:

- Establish IT hardware and software as supply system responsibility items (SSRI) or using unit responsibility items (UURI) (CD&I, I&L, MCSC: 90 days).
  - The program of record is responsible for SSRI budgeting, replacement, and end of life/end of service.
  - Commanders are responsible for UURI budgeting, replacement, and end of life/end of service.
- Develop recommendations for a *DOD Instruction 5000.02, Operation of the Defense Acquisition System* enclosure that focuses on rapid cyber acquisitions to be approved by USD AT&L's Cyber Investment Management Board (CD&I/MCSC: 60 days).
- Determine recommended changes to policy/regulations/statute.
- Recommend that Defense Acquisition University (DAU) update curriculum on *DOD 5000* and Department of Navy changes for rapid cyber acquisitions. (DAU: as soon as practicable).

Governance:

- Evaluate and streamline current Chief Information Officer Information Technology Procurement Review and Approval System (ITPRAS) processes and ensure alignment to the approved product list (C4: 60 days).
- Publish a Marine Corps order, replacing *MARADMIN 375/11, Information Technology (IT) Funding, Approval, and Procurement Policy*, to establish policy for IT funding, approval, and procurement (C4: 180 days).

• MCSC's technical authority and MARFORCYBER's directive authority for cyberspace operations will enforce engineering responsibilities to provide unified, standardized, configuration-controlled MCEN (MCSC/MFCC: Immediate).

In August 2016, the Commander, MCSC, issued another decision memorandum increasing the CAT's mission to a command cyber advisory team, and a year later, in June 2017, MCSC underwent a Force Structure Realignment that created a Principal Cyber Advisor (PCA). The PCA establishment is mirrored after the DOD's PCA and further increases the Command's emphasis on the need for culture change to one that understands and responds to cyber as operationalized IT. The PCA absorbed all previous cyber leadership responsibilities and added cybersecurity strategy and information environment responsibilities as a direct report to the Deputy to the Commander, Systems Engineering and Acquisition Logistics (DC, SEAL), also known as the chief engineer. The PCA has two liaison officers tasked with providing direct support to the Deputy Commandant, Information (DC, I), and to MFCC. The PCA's office consists of the PCA actual, two liaison officers, CAT, and a cyber-operations response team, which the Commander called for in July 2017 to provide the operational support and incident response function. The cyber-operations response team fielded the MCSC Program of Record Cyber Readiness Dashboard to provide a leadership portal informed with threat, risk, and vulnerability-based strategic information relevant to cyber stakeholders.

Rapid Cyber Acquisitions Process

The tailored rapid cyber acquisitions process addresses Marine Corps cyber needs. Per the 15 September 2015 Commander, MCSC's decision memorandum, the rapid cyber acquisitions process described below was effective immediately.

Key Terms

MCSC Rapid Cyber Acquisitions Process. A process specifically tailored for MCSC to execute emergency and urgent cyber requirements. Detailed process flow is provided in Figure 1 (see next page).

Emergency Cyber Requirement. A mission-critical requirement needed between 1 and 30 calendar days conveyed via the RTP using an urgent statement of need.

Urgent Cyber Requirement. A mission-critical requirement needed between 31 and 180 calendar days conveyed via the RTP using an urgent statement of need.

The CAT. A team comprised of command competency and program management office (PMO) subject-matter experts to plan, execute, and deliver materiel solutions for emergency and urgent cyber requirements. The CAT

will lead the acquisitions and fielding effort for emergency cyber requirements (less than 30 calendar days) and assist PMOs, as needed, with urgent cyber requirements (30 to 180 calendar days).

Rapid Cyber Acquisitions Approach

Emergency and urgent cyber requirements will be identified by CD&I via the urgent needs process and conveyed to MCSC via the RTP. The requirements transition team will pass the requirement to the CAT or PMO, depending on the level of urgency. CD&I shall clearly identify the urgency, priority, and source of funding relative to other requirements. The CAT will participate throughout the RTP to assist with the definition and acceptance of all cyber requirements.

The Rapid Cyber Acquisitions Process that the CAT developed to comply with the Commander's direction was built within the general acquisitions model framework contained in the current *DOD Instruction 5000.02, Operation of the Defense Acquisition System (Change 3)*. The tailored Rapid Cyber Acquisitions Process still conforms with all of the key activities that are associated with the traditional acquisitions model (eg., requirements definition, analysis of alternatives, product development, procurement, testing, and fielding). The primary key to success in implementing the Rapid Cyber Acquisitions Process is accelerating the review and approval times, as compared to the traditional acquisitions process, for required documentation and program review decisions. The process flowchart that illustrates the MCSC Rapid Cyber Acquisitions Process is provided in Figure 1.

In fall 2016, MCSC implemented the Rapid Cyber Acquisitions Process through an emergency procurement that was required in less than 30 days. After vetting the need and quickly putting the needed steps in place with leadership, a $100,000 materiel solution was fielded, the software was delivered in seven days, and the hardware delivered in 27 days. This small success demonstrated the validity of the acquisitions community's commitment to adapting the need of cyber speed. The intent is

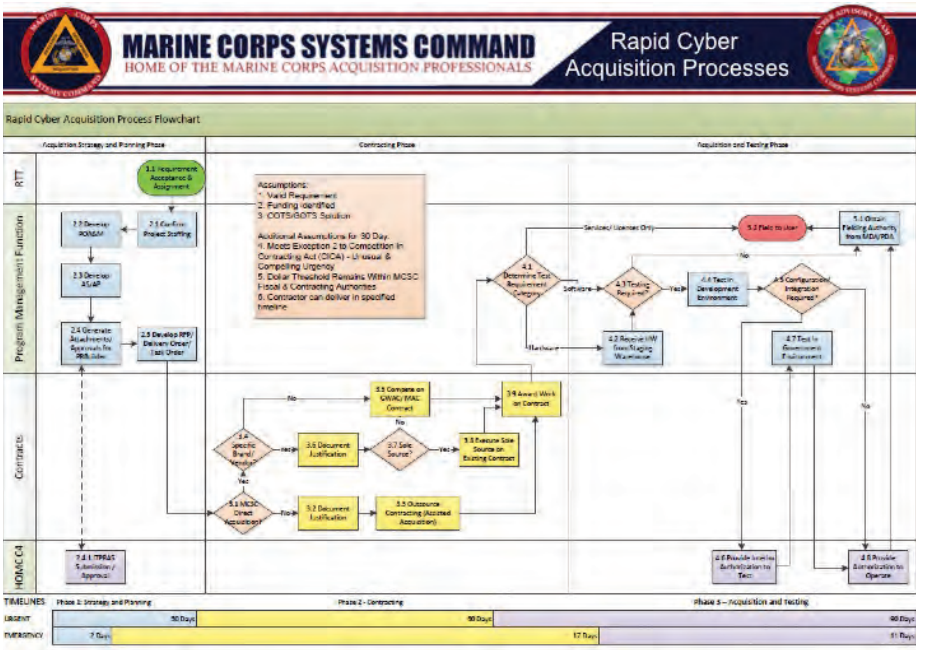

Figure 1.

for this example and others to provide the impetus for the Marine Corps' institutional stakeholders to come to grasp with the need to adapt their processes to meet the cyber pace. A key aspect of this adapatation is to fully implement the July 205 EOS-accepted recommendations to improve cyber/IT acquisitions.

The CAT will participate throughout the RTP to assist with the definition and acceptance of all cyber requirements.

MCSC continues to evolve cyber/IT acquisitions, and an aspect of this is MCSC's advocating for the decentralized execution of two currently stringently controlled IT processes and two traditionally focused enterprise management processes that cause latency in cyber/IT acquisitions. The two currently stringently controlled IT processes are the ITPRAS and the authorization official process, both of which are entirely controlled by a single office in HQMC, Director, C4. The other two processes that do not meet the pace of cyber are the requirements processes in DC, CD&I, and the budgeting process within DC, P&R. The second pair of processes is currently unable to meet the need at which cyber/IT acquisitions need to move, and the ITPRAS and authorization official processes could implement a delegated execution to add speed to cyber/IT acquisitions.

Other large-scale changes affecting Marine Corps acquisitions include the development and implementation of information environment operations as a component embedded within the National Defense Strategy. MCSC's Chief Engineer's PCA dedicates resources to supporting DC, I's concept of an objective network functioning as part of an inside force on the naval tactical grid. This concept is nascent, but the explorations are ongoing with additional process and procedural changes to come.

USMC