LETTER OF INSTRUCTION

From: Commandant of the Marine Corps

Subj: LETTER OF INSTRUCTION (LOI) MARINE CORPS COMMUNITY SERVICES (MCCS) ENTERPRISE NETWORK (MCCSNET) SYSTEM AND SERVICES ACQUISITION CONTROLS

Ref: (a) MCO 5239.2B, "Marine Corps Cybersecurity"
(b) CNSSI 1253, "Security Categorization and Control Selection for National Security Systems"
(c) NIST SP 800-53 "Security and Privacy Controls for Information Systems and Organizations"
(d) DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)"
(e) CNSSD 505, "Supply Chain Risk Management"
(g) MCO P1700.27B, "MCCS Policy Manual"
(h) MCO 7010.19, "MCCS Financial Management Procedures"
(i) MCO 4400.201, "Management of Property in the Possession of the Marine Corps"

1. Situation.

   a. This LOI prescribes policy, guidance, and responsibilities associated with the MCCS Enterprise Network (MCCSNet). The MCCSNet is comprised of the information technology (IT) assets, personnel, processes, and resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information within the MCCS enterprise, and is operated on the usmc-mccs.org network. The primary mission of the MCCSNet is to support the Marine Corps Exchange (MCX) and Morale Welfare and Recreation (MWR) programs operated by the MCCS enterprise.

   b. The MCCSNet is an unclassified part of the Marine Corps Cyberspace Environment (MCCE) and is governed by reference (a) and associated directives.

   c. The Deputy Commandant for Information (DCI), through the Director, Command, Control, Communications, Computers (C4) provides oversight of the MCCSNet. The Director C4, as the Marine Corps Chief Information Officer (CIO), is responsible for all Marine Corps systems and networks, provides governance, and establishes tasks, standards, and conditions for compliance, operations, and security for MCCSNet and other Marine Corps networks and enclaves. Marine Corps Forces Cyberspace Command (MARFORCYBER), acting through the Marine Corps Cybersecurity Operations Group (MCCOG), is the Cyber Security Service Provider (CSSP) for the MCCSNet.

   d. The Director, Business and Support Services Division (MR) has responsibility to DCI C4, MARFORCYBER, and MCCOG for ensuring the integrity
Subj: LETTER OF INSTRUCTION (LOI) MARINE CORPS COMMUNITY SERVICES (MCCS) ENTERPRISE NETWORK (MCCSNET) SYSTEM AND SERVICES ACQUISITION CONTROLS

of the MCCSNet and for ensuring compliance with all applicable policies. The MR Director exercises these responsibilities through the MR CIO, the MR Information System Security Manager (ISSM), and other designees.

e. All personnel with access to the MCCSNet have a fundamental responsibility for cybersecurity. Accordingly, all personnel with access to the MCCSNet will ensure compliance with policy referenced and established herein.

2. Mission. To ensure the integrity of the MCCSNet and to ensure that all MCCSNet IT solutions comply with applicable USMC, DON, and DoD cybersecurity policy.

3. Execution

a. Commander’s Intent

(1) Network Integrity. The MR CIO has responsibility for Supply Chain Risk Management (SCRM) of System and Services Acquisition controls pursuant to references (b), (c), (d), (e), and (f). This includes the procurement and the deployment of IT hardware and software hosted on or connected to the MCCSNet and IT contract services enabled through MCCS NAF procurement processes. The following definitions apply:

(a) IT Hardware. Tangible physical objects that are elements of a computer system, regardless of their physical location (i.e. cloud). Examples include servers, routers, switches, data storage, printers, laptops, smart phones, and virtual machines.

(b) IT Software. The non-physical part of a system that is installed or coded directly on IT hardware. Examples include minor applications, operating systems, firmware, desktop applications, and websites.

(c) IT Services. An agreement or plan to deliver, operate and/or control IT resources. Examples include web hosting, software development, application development, consulting, domain registrations, internet bandwidth, and cloud based services.

(2) Procurement Process. Installation Commanders, MCCS Directors, and MR Information Technology personnel must obtain approval through the MCCS IT Purchase Request (ITPR) process before procuring or implementing any new hardware, software, or IT contract services, regardless of the source or type of funds. The MR CIO uses the ITPR process to approve procurements of all hardware, software, or IT contract services. The MCCS ITPR process utilizes both the IT Procurement Review and Approval System (ITPRAS) directed by C4 and the MCCS electronic Purchase Request (ePR) system. ITPRs must be submitted to MR for all hardware (including peripherals and network infrastructure) or software that will be hosted on or connected to the MCCSNet, or IT contract services enabled through MCCS NAF procurement processes, including purchase card transactions.

(3) Property Control. MCCS Directors have custodial responsibilities for MCCS property in accordance with reference (g). All IT hardware must be
positively tracked and accounted for in a formal chain of custody process in accordance with reference (h) and (i). The property control process requires designated custodians to document all changes in custody including receipt, transfer, and disposal. The property accountability process ensures that MR knows what we own, where it is, and who has accountability and responsibility for each IT device.

b. Endstate. A secure MCCSNet, achieved through Supply Chain Risk Management, which is compliant with cybersecurity policies to ensure the confidentiality, integrity, and availability of MCCS information resources.

4. Tasks

a. Network Integrity. Installation Commanders, MCCS Directors, and MR Information Technology personnel will implement local procedures in compliance with MR ITPR guidance, to ensure that all new hardware, software, and IT contract services are reviewed and approved by the MR CIO before procurement or implementation on the network. MCCS Directors must ensure that MCCS personnel do not, without written approval by the MR Director, implement any new IT hardware, software, or IT contract services that have not been properly approved.

b. Procurement Process. Installation Commanders, MCCS Directors, and MR Information Technology personnel will ensure that IT Purchase Requests (ITPRs) are submitted to MR for all hardware, software, and IT contract services. Procurements made with the purchase card must be approved in advance through the ITPRAS/ePR process. Existing ITPRAS procedures will be used until updated MCCS ITPRAS policy and procedures are provided. All ITPRs will be prioritized and managed as directed by the MR CIO. Any hardware, software, or IT contract services implemented without authorization subsequent to this LOI, and discovered during auditing and testing by MR or MARFORCYBER, may be immediately deactivated.

c. Property Control. Installation Commanders, MCCS Directors, and MR Information Technology personnel will ensure all IT property, whether fixed assets or memo property, are positively tracked and accounted for in a formal custody process in accordance with reference (h) and (i). Designated property custodians will ensure compliance with existing policy using existing systems until updated MCCS property control policy and procedures are provided. MCCS Directors will ensure property records maintained in the MCCS Financial Management System are validated and remain current in preparation for migration to an automated property accountability system. MCCS Directors must prepare to conduct an inventory and document all IT devices, both fixed assets and memo property, procured or otherwise obtained by their activity.

5. Coordinating Instructions

a. The efforts required by this LOI are a high priority to protect MCCS assets from supply chain risks and to protect the privacy sensitive information of MCCS patrons and employees. Compliance requires the concerted commitment and support of all MCCS leadership and IT staff at MR, MF, and in the field.

b. Installation Commanders, MCCS Directors, and MR Information Technology personnel with responsibility for personnel with access to the MCCSNet will ensure compliance with all policy referenced and established
herein and ensure compliance with subsequent tasks and data calls in support of this initiative.

6. **Administration and Logistics**

   a. The Deputy Director, CIO (MR), will direct the actions defined within this LOI. Questions should be directed to Mr. Jerry Burkett, IT Program Manager at burkettf@usmc-mccs.org.

   b. MR will communicate task status to the Information Technology Committee as needed.

   c. This LOI has been coordinated with DCI C4, MCCOG, and MCICOM.

7. **Command and Signal**

   a. Command. This LOI is applicable to all MCCS activities.

   b. Signal. This LOI is effective on the date signed.

   David J. Turner
   Director (acting)
   Business and Support
   Services Division

Distribution:
COMMARFORCOM
CG MCCDC
CG TECOM
COMMCMICOM
CG MCIPAC
CG MCWEST
CG MCIEAST
CG MCRD/WRR
CG MCAGCC
CG MCRD/ERR
DIR C4
DIR MARFORCYBER
DIR MCCOG
CO MCINCR/MCB Quantico
CO Camp Allen
CO H&S Bn HQMC
CO MARBKS 8TH & I
CO MCAS Beaufort
CO MCAS Cherry Point
CO MCAS Iwakuni
CO MCAS Miramar
CO MCAS New River
CO MCAS Yuma
CO MCB Hawaii
CO MCLB Albany
CO MCLB Barstow
CO 1st MCD
CO MCSFBn Bangor