



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3044 CATLIN AVENUE
QUANTICO, VIRGINIA 22134-5103

IN REPLY REFER TO:
1700
MRI
APR 03 2018

LETTER OF INSTRUCTION

From: Commandant of the Marine Corps

Subj: LETTER OF INSTRUCTION (LOI) MARINE CORPS COMMUNITY
SERVICES (MCCS) CYBERSECURITY FOR COMMERCIAL WIRELESS
INTERNET SERVICES

Ref: (a) MCO 5239.2B
(b) SECNAVINST 5211.5E
(c) MCO 7010.20

Encl: (1) Commercial Wireless Internet Security Requirements

1. Situation

a. This LOI prescribes policy, guidance, and responsibilities associated with MCCS information systems, referred to as the MCCS Enterprise Network (MCCSNet). The MCCSNet is comprised of the information technology assets, personnel, processes, and resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information within the MCCS enterprise, primarily 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 of the MCCSNet and for ensuring compliance with all applicable policies. The MR Director exercises these responsibilities

Subj: LETTER OF INSTRUCTION (LOI) MCCS CYBERSECURITY FOR
COMMERCIAL WIRELESS INTERNET SERVICES

through the MR Chief Information Officer (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 the references and policy established herein.

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

3. Execution

a. Commander's Intent. Installation MCCS Directors may acquire commercial wireless internet capabilities for MCCS facilities when such capabilities meet certain cybersecurity requirements.

(1) All commercial wireless internet access acquired through NAF procurement processes must meet the cybersecurity requirements prescribed by DCI C4 as detailed in enclosure (1).

(2) All commercial wireless internet access acquired through NAF procurement processes must be locally coordinated with the installation G6/S6.

b. Endstate. A secure MCCSNet that is compliant with cybersecurity policies to ensure the confidentiality, integrity, and availability of MCCS information resources.

4. Tasks

a. MCCS Directors must:

(1) Ensure MCCS personnel do not enter into new contracts or execute options or modifications of existing contracts, or any other procurement action that is subject to reference (c), that could result in the implementation of wireless internet service except when such services comply with the cybersecurity requirements prescribed by DCI C4. Requests for exceptions must be forwarded to CMC (MR).

(2) Ensure commercial wireless internet services are not connected to the MCCSNet.

(3) Ensure official government business is not conducted using commercial wireless internet service.

(4) Submit a formal response if they intend to opt out of the MCCS enterprise wireless contract. The response should be submitted using DON Tracker within three weeks of the date of this LOI and

Subj: LETTER OF INSTRUCTION (LOI) MCCS CYBERSECURITY FOR
COMMERCIAL WIRELESS INTERNET SERVICES

should be addressed to Ms. Lynn Davis, Head, NAF Procurement Branch (MRB).

(5) Identify existing commercial wireless internet services, whether by NAF contract or service agreement, and provide a remediation plan to bring all such services into compliance with the cybersecurity requirements prescribed by C4. Remediation of existing noncompliant contracts must be completed no later than 30 September 2018. The response, detailing existing wireless services and the associated remediation plans, is due to MR 30 days from the date of this LOI. The responses should be submitted using DON Tracker and addressed to Ms. Gabbie Bowie (MRI), Mr. Gary Gresham (MRI), and Ms. Lynn Davis (MRB).

b. The MR CIO will monitor the remediation plans, maintain current cybersecurity requirements on the SharePoint site, and periodically inspect for MCCSNet compliance.

5. Coordinating Instructions

a. MR will provide guidance to NAF Regional Procurement Offices to coordinate the NAF procurement actions required for remediation and for future NAF procurements.

b. Installation Commanders and MCCS leaders will coordinate with installation G6/S6 for all requirements development and project approvals. Installation G6/S6 is responsible for:

(1) Planning or providing for the initial circuit termination, distribution, and delivery of networks within and between facilities and training areas.

(2) Coordinating and approving any adds, moves, and changes to telecom infrastructure, including internal cable plant and wireless access points.

(3) Managing any and all circuits and networks terminating or traversing through the installation.

c. Installation Commanders and MCCS leaders may purchase service for additional sites through the enterprise wireless contract under the applicable contract pricing schedule. Coordination of additional sites should be made with Ms. Lynn Davis (MRB) through the appropriate Regional Procurement Office.

d. Installation Commanders and MCCS leaders with responsibility for personnel with access to the MCCSNet will ensure compliance with the references, this LOI, and subsequent tasks and data calls in support of this initiative.

Subj: LETTER OF INSTRUCTION (LOI) MCCS CYBERSECURITY FOR
COMMERCIAL WIRELESS INTERNET SERVICES

6. Administration and Logistics

a. The Deputy Director, CIO (MR), and Deputy Director, Support will coordinate the actions defined within this LOI. The project lead and POC is Ms. Gabbie Bowie: cybersecurity@usmc-mccs.org.

b. MCCS Directors will designate a project lead to coordinate execution of the tasks in this LOI when responding to this tasker. This project lead will typically be the installation MCCS MIS Coordinator in coordination with NAF procurement personnel.

c. CMC (MR) will communicate task status to the Information Technology Committee as needed.

d. This LOI has been coordinated with DCI C4 and COMMCICOM.

7. Command and Signal

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

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


CINDY WHITMAN LACY
Director
Business and Support Services
Division

Distribution:

COMMARFORCOM	CO MCAS New River
CG MCCDC	CO MCAS Yuma
CG TECOM	CO MCB Hawaii
COMMCICOM	CO MCLB Albany
CG MCIPAC	CO MCLB Barstow
CG MCIWEST	CO 1 st MCD
CG MCIEAST	CO MCSFBn Bangor
CG MCRD/WRR	MCCS MCICOM
CG MCAGCC	MCCS MCIEAST, MCB Lejeune
CG MCRD/ERR	MCCS MCIWEST, MCB Pendleton
DIR C4	MCCS MCIPAC, MCB Butler
DIR MARFORCYBER	AC/S MCCS MCRD/WRR
DIR MCCOG	AC/S MCCS MCAGCC
CO MCINCR/MCB Quantico	MCCS Dir Camp Allen
CO Camp Allen	MCCS Dir H&S Bn HQMC
CO H&S Bn HQMC	MCCS Dir MARBKS 8th & I
CO MARBKS 8TH & I	MCCS Dir MARFORCOM
CO MCAS Beaufort	MCCS Dir MARFORPAC
CO MCAS Cherry Point	MCCS Dir MARFORRES
CO MCAS Iwakuni	MCCS Dir MCAS Cherry Point
CO MCAS Miramar	MCCS Dir MCAS Iwakuni

Subj: LETTER OF INSTRUCTION (LOI) MCCS CYBERSECURITY FOR
COMMERCIAL WIRELESS INTERNET SERVICES

MCCS Dir MCAS Miramar
MCCS Dir MCAS Yuma
MCCS Dir MCB CLNC/NR
MCCS Dir MCB CPEN/BAR

MCCS Dir MCB Hawaii
MCCS Dir MCB Quantico
MCCS Dir MCLB Albany
MCCS Dir South Carolina