UPDATE 1: U.S. MARINE CORPS ENTERPRISE NETWORK REMOTE ACCESS PREPAREDNESS PLANNING GUIDANCE

Date Signed: 3/17/2020 | MARADMINS Number: 170/20

MARADMINS : 170/20

R 171616Z MAR 20
MARADMIN 170/20
MSGID/GENADMIN/CMC DCI IC4 WASHINGTON DC SUBJ/UPDATE 1: U.S. MARINE CORPS ENTERPRISE NETWORK REMOTE ACCESS PREPAREDNESS PLANNING GUIDANCE//
REF/A/MSG/MARADMIN 156/20 111257Z MAR 20//
REF/B/MSG/MARADMIN 167/20 140450Z MAR 20//
REF/C/MSG/MCO 12271.1/20180905//
REF/D/DOC/PA 1974/USC/31DEC1974//
REF/E/DOC/EO 9397/USG/20NOV2008//
REF/F/DOC/DOD 5400.11-R/DOD/14MAY2007//
REF/G/DOC/SECNAVI 5211.5E/DON/28DEC2005//
REF/H/DOC/ SECNAVM 5210.1/DON/16NOV2007//
REF/I/DOC/ECSM 011/DCI/30APR2013//
REF/J/MSG/MARADMIN 496/19//
NARR/REF A IS MARADMIN 156/20 U.S. MARINE CORPS ENTERPRISE NETWORK REMOTE ACCESS PREPAREDNESS PLANNING GUIDANCE. REF B IS MARADMIN 167/20 UPDATE #3: U.S MARINE CORPS DISEASE CONTAINMENT PREPAREDNESS PLANNING GUIDANCE FOR 2019 NOVEL CORONAVIRUS (COVID-19); STOP MOVEMENT. REF C IS MCO 12271 TELEWORK FOR CIVILIAN MARINES. REF D is the Privacy Act of 1974. REF E is Executive Order 9397, Federal Use of Social Security Numbers With Amendments. REF F is Department of Defense Privacy Program. REF G is Secretary of the Navy Instruction 5211.5E, Department of the Navy (DON) Privacy Program. REF H Secretary of the Navy Manual 5210.1, Department of the Navy Records Management Manual. REF I is ECSM 011 Personally

Identifiable Information (PII), Marine Corps policy for the handling and management of PII data. REF J IS MARADMIN 496/19 DOD SAFE ACCESS FILE EXCHANGE (SAFE) USAGE IN THE MARINE CORPS.//
POC/CARLOS URBINA/COL/UNIT: DC I IC4/TEL: (571) 256-9062/NIPR E-MAIL: CARLOS.URBINA@USMC.MIL//
POC/MICHAEL SCHWEIGHARDT/CIV/UNIT: DC I IC4/TEL: (571) 256-8819/NIPR E-MAIL: MICHAEL.SCHWEIGHARDT@USMC.MIL//
GENTEXT/REMARKS/1. This MARADMIN updates original guidance in MARADMIN 156/20 (reference A) on the use of resources available for remote access to the Marine Corps Enterprise Network (MCEN).
1.A. Background. Per reference B, the Marine Corps has implemented guidance to protect the force while executing the Marine Corps' mission during the Corona Virus Disease-19 (COVID-19) outbreak.
2. Mission. The Marine Corps will utilize the MCEN remote access resources outlined in MARADMIN 156/20 in a manner which enables effective and efficient mission execution.
3. Execution.
3.A. Concept of operations. The Deputy Commandant for Information, in coordination with Marine Corps Forces Cyberspace Command (MFCC), will optimize MCEN capabilities along two lines of effort (LOE) in support of Marine Corps mission requirements for dispersed operations during COVID-19.
3.A.1. LOE 1 – Network capability awareness, prioritized network access, and resource optimization. Actions in this LOE focus on maximizing user awareness of available MCEN remote access capabilities, as well as education on the use of those resources. The endstate is assured access and sufficient bandwidth in support of personnel performing mission essential functions.
3.A.2. LOE 2 – Expansion of MCEN remote access capability and capacity. Concurrent with LOE 1 actions, DC I and MFCC are working with the Department of Defense (DoD) and Department of the Navy (DoN) Chief Information Officer (CIO) to expand current MCEN remote access resources. The endstate is the expansion of current Outlook Web Access (OWA) and Virtual Private Network (VPN) capacity, as well as exploration of additional collaboration tools.
3.B. Tasks. Commanders will:
3.B.1. Maximize the use of Marine Corps issued mobile devices for MCEN remote access by personnel who have been issued those devices (ie. Samsung or iPhone).
3.B.2. Use OWA as the primary means for remote access to the MCEN to

support mission requirements. OWA is accessible from any computer with an Internet connection and a Common Access Card reader.
3.B.2.A. Ensure personnel reduce the amount of emails resident in their mailbox in preparation for remote access operations, to include movement of emails to .PST files. This action will reduce the likelihood that a user may exceed their mailbox size limit.
3.B.2.B. Ensure personnel minimize the use of large attachments to the maximum extent possible in order to prevent exceeding mailbox size limits. Mailbox size limitations for designated VIP users have already been increased, in accordance with DC I network policies.
3.B.3. Reserve the use of VPN via Pulse Secure remote access for only those personnel with the mission requirement to access full email services, shared drives, command SharePoint pages, and business applications. Due to MCEN Pulse Secure capacity limitations, personnel will be automatically removed after 1-2 hours of connectivity to ensure additional users are also able to achieve mission requirements. Users are encouraged to work offline to the maximum extent possible. Personnel must disconnect from Pulse Secure when continuous connectivity is not necessary. Designated VIP users will have full access to these services.
3.B.4. Ensure appropriate protections for government information and personally identifiable information (PII). Government records taken from a worksite to an alternate location require safeguard under federal law, as well as DoD, DoN and USMC policy. The Privacy Act expressly requires that PII be secured. Marine Corps personnel accessing PII outside government workspaces must comply with references (D-I) to protect the privacy of sensitive records. Hard copy documents containing PII must be inventoried before removal from the government worksite. In case of a PII incident, all reporting requirements outlined in reference (I) must be followed within the prescribed timelines.
3.B.5. Per reference (J), utilize the Department of Defense Safe Access File Exchange (SAFE) site in order to securely transfer Marine Corps unclassified and sensitive data. The SAFE site is available at https: (slash)(slash)safe.apps.mil/
3.C. Coordinating instructions.
3.C.1. In accordance with LOE 2, the Marine Corps is pursuing additional MCEN remote access capability and capacity. Additional guidance will be published as additional resources become available.
3.C.2. The MCEN User Portal contains a Self-Help section under the Self Service Tab. The Self-Help section contains information to assist users in the operation of capabilities provided on the MCEN, to include “How To”

guides. The MCEN User Portal is located at: https: (slash) (slash)homeport.usmc.mil/SitePages/home.aspx
3.C.3. Instructions on how to encrypt or decrypt OWA messages using S/MIME are available at: https: (slash)(slash)support.office.com/en-us/article/encrypt-messages-by-using-s-mime-in-outlook-on-the-web-878c79fc-7088-4b39-966f-14512658f480
4. Administration and logistics. Assistance with MCEN capabilities is available via command G-6/S-6 personnel. For additional assistance contact the Enterprise Service Desk at 855-373-8762.
5. Command and signal.
5.A. Command. This MARADMIN applies to the Total Force.
5.B. Signal. This MARADMIN is effective upon release. Ensure widest dissemination.
6. Release authorized by BGen L. M. Mahlock, Director, Information C4 Division, Deputy Commandant for Information.//