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

Date Signed: 3/11/2020 | MARADMINS Number: 156/20

R 111257Z MAR 20
MARADMIN 156/20
MSGID/GENADMIN/CMC C FOUR WASHINGTON DC//
SUBJ/U.S. MARINE CORPS ENTERPRISE NETWORK REMOTE ACCESS PREPAREDNESS PLANNING GUIDANCE//
REF/A/DOC/MEMORANDUM/UNDER SECRETARY OF THE NAVY/12JUL19//
REF/B/MSG/MARADMIN 432/19 071608Z AUG 19//
NARR/REF A IS THE UNDER SECRETARY OF THE NAVY MEMO TO THE DON REITERATING THE PROHIBITION AGAINST USING NON-OFFICIAL, PERSONAL MESSAGING ACCOUNTS TO CONDUCT OFFICIAL BUSINESS. REF B IS MARADMIN 432/19 USE OF PERSONAL MESSAGING ACCOUNTS TO CONDUCT OFFICIAL BUSINESS//
POC/MICHAEL SCHWEIGHARDT/CIV/UNIT: DC I IC4/TEL: (571) 256-8819/NIPR E-MAIL: MICHAEL.SCHWEIGHARDT@USMC.MIL//
GENTEXT/REMARKS/1. When authorized by appropriate command authority, personnel may be directed to work at an alternate work location or telework. This message provides information on capabilities available to users that may need to work from an alternate location.
2. Outlook Web Access (OWA). OWA is a Common Access Card (CAC)-enabled, web-based email client with the look and feel of the Outlook client. OWA allows users access to their mailboxes and calendars from any Internet connection regardless of whether or not the computer is equipped with Outlook. OWA can be accessed at https:(slash)(slash)owa.usmc.mil. Users that are part of the Office 365 pilot can access OWA at https:(slash)(slash)O365.usmc.mil
3. Virtual Private Network (VPN). Pulse Secure VPN software provides remote and mobile

users with secure, authenticated access to Marine Corps Enterprise Network (MCEN) Non-secure Internet Protocol Router Network (NIPRNet) e-mail services, shared drives, and business applications. Pulse Secure access is available from Marine Corps-issued NIPRNet devices and must be preconfigured before use, to include enabling of the wireless fidelity (Wi-Fi) capability. Detailed instructions for use of the Pulse Secure VPN software is available at https: (slash)(slash)eris.mceits.usmc.mil/arsys(slash) (slash)forms/ars9.mceits.mcw.ad.usmc.mil/RKM%3AKnowledgeArticleManager/Display+View/?eid=KBA000000039601&cacheid=84eb1bf9

4. Defense Collaboration Services (DCS). DCS provides secure web conferencing and instant messaging services on the NIPRNet, and is accessible via the Internet. DCS resides on milCloud, a datacenter virtualized hosting environment, and supports CAC and select hard token holders and guest (DoD mission partners) users. DCS can be accessed at https:(slash) (slash)disa.mil/Enterprise-Services/Applications/Defense-Collaboration-Services

5. DoD Mobility Classified Capability - Secret (DMCC-S). DMCC-S is an enterprise service that enables government owned mobile devices access to the Classified Secret Department of Defense Information Network (DoDIN) telephony and information services. DMCC-S is available to select senior personnel in coordination with this headquarters via the Information Technology Procurement Request System (ITPRS). For additional device information, please visit the DOD Mobility User Portal at https:(slash)(slash)storefront.disa.mil/kinetic/disa/service-catalog#/forms/dod-mobility-classified-capability---secret

6. Per the references, this MARADMIN reiterates the mandate to use DoD messaging accounts to conduct official business. The use of non-official, personal messaging accounts to conduct official business is strictly prohibited.

6.a. All Marines, Marine Corps officials, and Marine Corps employees are required to understand and comply with the references, which mandate the use of official messaging accounts to conduct official business, to better ensure the security of government information and transparency of official Marine Corps business.

6.b. All Marines, Marine Corps officials, and Marine Corps employees are responsible for properly protecting government information that they access, create, or transmit.

6.c. All Marines, Marine Corps officials, and Marine Corps employees are required to understand the regulations for proper handling of classified information, controlled unclassified information, and non-public government information.

7. Users are reminded that in the event that a large number of personnel are performing duties from an alternate work location or teleworking, they may experience delays due to the high volume of personnel using the limited remote access points.

8. For additional assistance contact the Enterprise Service Desk at 855-373-8762. Additional information is available at the MCEN User Portal at https:(slash) (slash)homeport.usmc.mil/SitePages/home.aspx

9. Release authorized by BGen L. M. Mahlock, Director, Information C4 Division, Deputy Commandant for Information.//