REVIEW OF ONLINE PERSONAL INFORMATION AND HABITS

Date Signed: 4/1/2015
MARADMINS Active Number: 173/15

R 012035Z APR 15
MARADMIN 173/15
MSGID/GENADMIN/CMC WASHINGTON DC DMCS(UC)//
SUBJ/REVIEW OF ONLINE PERSONAL INFORMATION AND HABITS//
REF/A/DOC/SECNAV WASHINGTON DC CHINFO/21FEB2012//
REF/B/DOC/HQMC WASHINGTON DC C4 IA/9APR2009//
NARR/REF A IS SECNAVINST 5720.44C CH-1, DEPARTMENT OF THE NAVY PUBLIC AFFAIRS POLICY AND REGULATIONS. REF B IS HQMC ENTERPRISE INFORMATION ASSURANCE DIRECTIVE 011, PERSONNALLY IDENTIFIABLE INFORMATION (PII).//
POC/JAMES CAIN/CIV/DC PPO PSS/-/TEL:COML (703) 695-7203/EMAIL: JAMES.M.CAIN1(AT) USMC.MIL//
POC/JOHN CALDWELL/LTCOL/OMCC PA/-/TEL:COMM (703) 614-4309/EMAIL: ONTHERECORD(AT) USMC.MIL//
GENTEXT/REMARKS/1. THE ISLAMIC STATE IN IRAQ AND THE LEVANT (ISIL) RECENTLY PUBLISHED A LIST CONTAINING THE NAMES, PHOTOS AND ALLEGED ADDRESSES OF ROUGHLY 100 U.S. MILITARY PERSONNEL AND A CALL "TO KILL THEM IN THEIR OWN LANDS." THE NAVAL CRIMINAL INVESTIGATIVE SERVICE (NCIS) IS ACTIVELY EVALUATING THIS THREAT AND WORKING WITH LAW ENFORCEMENT AND U.S. INTELLIGENCE PARTNERS TO ADDRESS THIS INCIDENT. NCIS NOTIFIED ALL AFFECTED NAVY AND MARINE CORPS SERVICE MEMBERS AND THEIR FAMILY MEMBERS AS QUICKLY AS POSSIBLE. NCIS AGENTS ALSO PROVIDED GUIDANCE ON PERSONAL PROTECTION AND INCREASING THEIR VIGILANCE AND AWARENESS. NCIS CONTINUES TO WORK WITH OTHER AGENCIES TO REDUCE THE EFFECTS OF THESE THREATS.
2. THE DATA ISIL RETRIEVED ON SERVICE MEMBERS WAS NOT THE RESULT OF HACKING INTO DEPARTMENT OF DEFENSE NETWORKS, IT WAS OBTAINED FROM PUBLIC INTERNET SITES. ISIL THEN USED THIS DATA AS A FORM OF INTERNET HARASSMENT CALLED DOXXING, WHICH IS THE PRACTICE OF REVEALING PERSONAL, PRIVATE, OR IDENTIFYING INFORMATION ABOUT PEOPLE ONLINE FOR VARIOUS REASONS SUCH AS EXTORTION, COERCION, HARASSMENT, PUBLIC SHAMING AND VIGILANTE JUSTICE.
3. COMMANDERS ARE RESPONSIBLE TO EDUCATE THEIR MARINES, CIVILIANS, CONTRACTORS, AND FAMILY MEMBERS ON THE BENEFIT OF ROUTINELY REVIEWING THEIR ONLINE AND SOCIAL MEDIA PRESENCE AND BEHAVIOR. MARINE CORPS LEADERSHIP HAS NO INTENT TO RESTRICT THE USE OF SOCIAL MEDIA OR ONLINE ACTIVITIES THAT ARE COMPLIANT WITH EXISTING POLICY, ONLY TO PREVENT EXPLOITATION OF DATA RESIDING ONLINE OR ON SOCIAL PLATFORMS. THE MARINE CORPS MAINTAINS AN ONLINE AND COMPREHENSIVE HANDBOOK ENTITLED "THE SOCIAL CORPS." THE INTENT OF THIS HANDBOOK IS TO OUTLINE HOW OUR CORE VALUES SHOULD BE DEMONSTRATED ONLINE AND TO GUIDE MARINES THROUGH THE USE OF SOCIAL MEDIA, WHETHER IN A PERSONAL CAPACITY OR WHEN ACTING ON BEHALF OF THE MARINE CORPS. THIS HANDBOOK, ALONG WITH COMPREHENSIVE SOCIAL MEDIA GUIDANCE, CAN BE FOUND AT THE FOLLOWING WEB ADDRESS: HTTP:(SLASH SLASH) WWW.MARINES.MIL/NEWS/SOCIALMEDIA.ASPX.
4. COMMANDERS WILL IMMEDIATELY TAKE THE FOLLOWING ACTIONS TO INCREASE ONLINE OPERATIONAL SECURITY (OPSEC) AWARENESS IN THEIR COMMANDS.
A. ENSURE COMPLIANCE WITH REFERENCE A REGARDING COMMAND/UNIT SOCIAL MEDIA PAGES, WEBSITES, BIOGRAPHIES, ETC, FOR CONTENT AND OPSEC CONCERNS. EXISTING PUBLIC AFFAIRS GUIDANCE REGARDING THE RELEASE OF INFORMATION REMAINS IN EFFECT.
B. DIRECT ALL PERSONNEL TO REVIEW THEIR ONLINE FOOTPRINT AND SOCIAL MEDIA ACCOUNTS FOR CONTENT AND PRIVACY SETTINGS (E.G., CONDUCT AN ONLINE SEARCH FOR PERSONAL INFORMATION, OR ANY INFORMATION THAT MIGHT COMPROMISE OPSEC). PERSONNEL SHOULD ATTEMPT TO REMOVE OR OTHERWISE RENDER INACCESSIBLE POTENTIALLY SENSITIVE INFORMATION. IF PERSONAL REMEDIATION ACTIONS AND PLATFORM CUSTOMER SERVICE PROVE INEFFECTIVE, NOTIFY YOUR CHAIN OF COMMAND. COMMANDERS SHOULD REQUEST ASSISTANCE VIA OPSEC AND PERSONALLY IDENTIFIABLE INFORMATION (PII) CHANNELS, STAFF JUDGE ADVOCATE, OR LAW ENFORCEMENT OFFICIALS, AS APPROPRIATE.
C. IN ACCORDANCE WITH THE REFERENCES AND NOTED ONLINE RESOURCES, COMMANDERS SHOULD REITERATE THAT MARINES ARE ENCOURAGED TO MAKE PERSONAL, UNOFFICIAL POSTS REGARDING THE MARINE CORPS AND MARINE CORPS-RELATED TOPICS RELATED TO THEIR PROFESSIONAL EXPERTISE, PERSONAL EXPERIENCES, OR PERSONAL KNOWLEDGE. MARINES SHALL NOT POST CLASSIFIED, CONTROLLED UNCLASSIFIED INFORMATION (CUI), OR SENSITIVE INFORMATION (FOR EXAMPLE, TACTICS, TROOP MOVEMENTS, FORCE SIZE, WEAPON SYSTEM DETAILS, ETC). MARINES SHOULD BE EXTREMELY MINDFUL WHEN DISCLOSING PERSONAL DETAILS ON THE INTERNET, AND SHOULD NOT RELEASE PII. EXAMPLES OF PII INCLUDE A MARINE'S HOME ADDRESS, BIRTHDAY, BIRTH PLACE, ETC. SPECIFIC PII GUIDANCE CAN BE FOUND IN REFERENCE B. WHEN IN DOUBT, MARINES SHOULD CONTACT THEIR UNIT'S OPERATIONS OFFICER, SECURITY OFFICER, INTELLIGENCE OFFICER, OR PUBLIC AFFAIRS OFFICER FOR GUIDANCE.
5. SOCIAL MEDIA IS AN INVALUABLE TOOL FOR INFORMATION SHARING, BUT IT MUST BE USED IN A RESPONSIBLE MANNER IF WE ARE TO PROTECT OUR MARINES, SAILORS, CIVILIANS, AND FAMILY MEMBERS, AND SAFEGUARD THE MISSION.
6. RELEASE AUTHORIZED BY LIEUTENANT GENERAL JAMES B. LASTER, DIRECTOR, MARINE CORPS STAFF.//